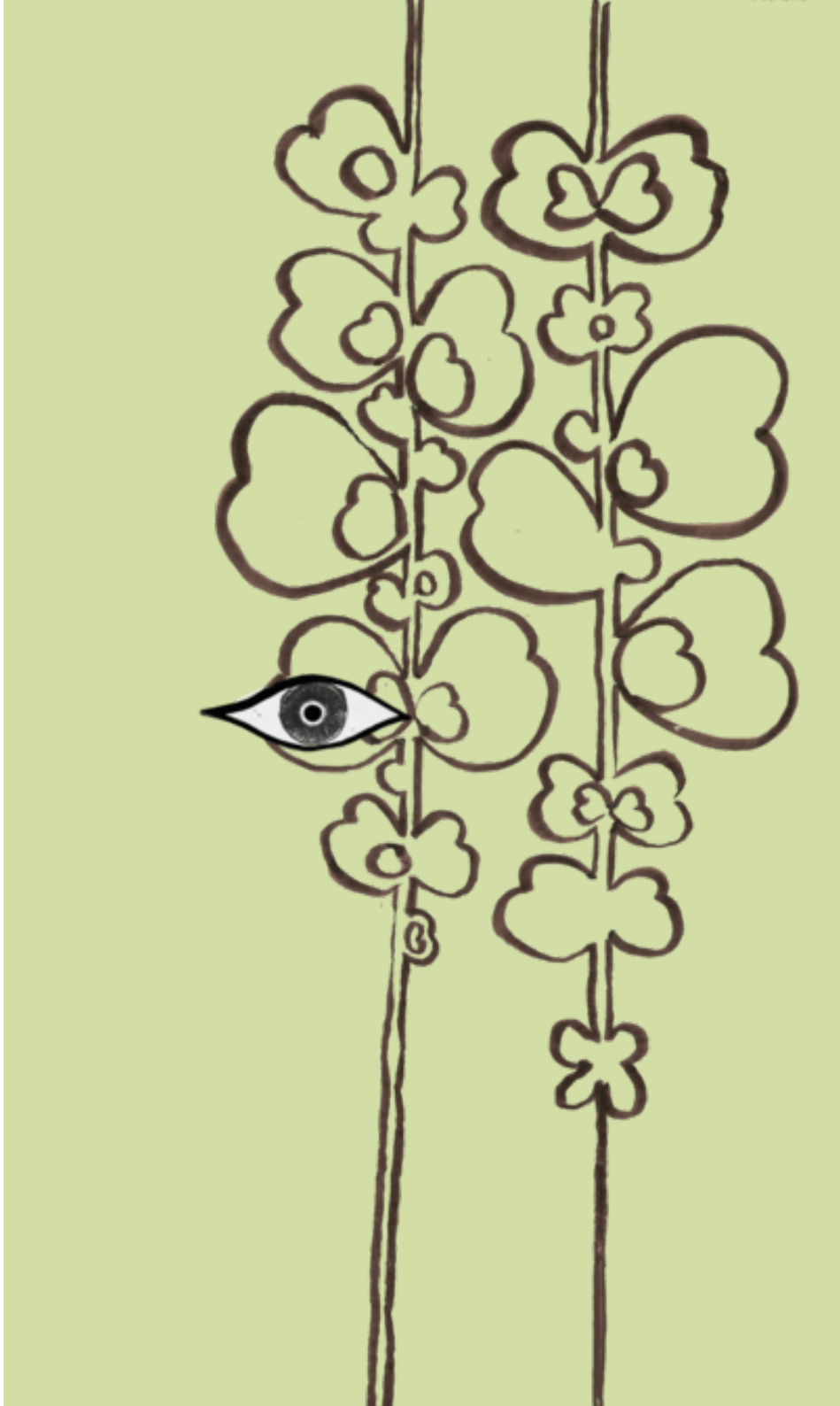
security in-a-box

عُدَّة الأمان

أدوات وممارسات للأمان الرقمي

الإصدارة ٠,٩,٠٦



عدة الأمان أنتجتها Tactical Tech و Front Line بمشاركة من :

التنسيق والكتابة والتحرير	Wojtek Bogusz Dmitri Vitaliev Chris Walker
الكتابة الإضافية	Cormac McGuire Benji Pereira
مراجعة الإنجليزية والتنضيد	Caroline Kraabel Benji Pereira
اختبار القراءة	Rosemary Warner
التصميم البصري	Lynne Stuart
تنسيق أقلمة البرمجيات	Louise Berthilson Alberto Escudero Pascual
فريق العربية	
التحرير والترجمة والأقلمة	أحمد غربية
التحرير	منال حسن
الترجمة والأقلمة والتنضيد	خالد حسني
الترجمة	محمد فتحي كلفت
فريق الفرنسية	
التحرير والترجمة والأقلمة	Patrick Cadorette
الترجمة والأقلمة	Alexandre Guédon
المراجعة	Miriam Heap-Lalonde
التحرير	Fabian Rodriguez
فريق الإسبانية	
الترجمة	Phol Edward Paucar Aguirre
التحرير	Katitza Rodríguez Pereda
إدارة الموقع	Angelin Venegas Ramírez
الأقلمة	Diego Escalante Urrelo
المراجعة	Carlos Wertheman
فريق الروسية	
الترجمة	Emin Akhundov
الترجمة	Alexei Bebinov
الترجمة	Alexander Lapidus
المراجعة	Ksenia Shiryaeva
التحرير والترجمة والأقلمة	Sergei Smirnov
شكر خاص لكل من	Robert Guerra و The Citizen Lab و Internews و Riseup ومشروع Tor و VaultletSoft
التمويل	Hivos people unlimited

الفهرس

مقدمة

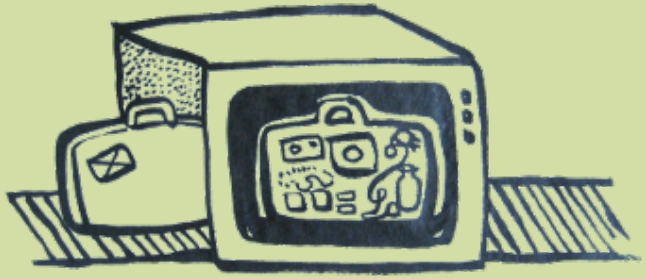
يتناول هذا الدليل موضوعات ومفاهيم ينبغي الإلمام بها لتحسين الأمان والسرية أثناء استخدام أدوات تقنية المعلوماتية، وهو يعدد ويشرح المخاطر التي تواجهك ويعينك على اتخاذ قرار رشيد في كيفية تقليل تلك المخاطر، ولأجل هذا فهي تغطي ثمانية موضوعات عامة تتعلق بالأمان وحماية البيانات وخصوصية الاتصالات.

في مقدمة كل فصل يوجد سيناريو تطبيقي فيه شخصيات خيالية تظهر في حوارات قصيرة عبر الفصل لتوضيح نقاط محددة وإثارة أسئلة شائعة. توجد كذلك قائمة موجزة بأهداف الفصل من المفيد إلقاء نظرة سريعة عليها قبل مواصلة القراءة. أثناء القراءة ستجد مصطلحات تقنية تربط كل منها إلى مُدخلة تشرحها في معجم، كما ستجد إحالات إلى برمجيات مشروحة في دليل الأدوات.

كل فصل في أي من الدليلين يمكن قراءته بمعزل عما سواه، كما توجد من كل فصل نسخة منسقة بما يناسب الطباعة، ويمكن البدء من أي موضع في كل دليل واتِّباع الروابط والإحالات كيفما يناسبك، إلا أن الفائدة تكون أشمل إن قرأت فصول هذا الدليل بالترتيب، إذ أن ممارسات الأمان تنبني كل منها على الأخرى، ومن غير المجدي مثلا أن تقفز إلى وسائل تأمين سرية المراسلات في الوقت الذي فيه تقبع في حاسوبك برمجيات تجسسية تُسجِّل كل ما تفعله لحساب طرف آخر ! لا نعني بهذا أن أيا من الجوانب أهم من الأخرى، إلا أن الموضوعات اللاحقة تقوم على افتراضات عمّا تعرفه وعن درجة أمان النظام التي تعمل فيه.

مع هذا توجد مبررات وجيهة لرغبتك في مطالعة الفصول بغير ترتيبها، فقد تريد مثلا معرفة كيفية إجراء حفظ احتياطي لبياناتك الهامة قبل البدء بتنصيب واستخدام الأدوات المشروحة في الفصول الأخرى ؛ كما قد تكون في حالٍ تواجهك فيه أزمة طارئة تستوجب حماية البيانات الحساسة المحفوظة في حاسوبك، أو قد تعمل من مقهى الإنترنت على حاسوب لا تهتم بسلامته ولا تنوي استخدامه للعمل على بيانات حساسة إلا أنك تودُّ معرفة كيفية الحفاظ على مجهوليتك أثناء تصفح موقع ما، أو كيفية تجاوز الحجب المفروض على موقع.

١
حماية الحاسوب من البرمجيات الخبيثة ومن المخترقين



١. حماية الحاسوب من البرمجيات الخبيثة ومن المخترقين

أيًا كانت طبيعة عملك فإن المحافظة على سلامة الحاسوب هي الخطوة الأولى على درب المحافظة على الخصوصية. لذا فقبل أن تَشغَل بالك بكلمات السر وتأمين الاتصالات والمحو الآمن وغيرها من موضوعات، عليك التيقن من أن الحاسوب الذي تعمل عليه ليس عرضة لهجمات **المخترقين** أو موبوءا **بالبرمجيات الخبيثة** مثل الفيروسات وأحصنة طروادة والبرمجيات التجسسية. بغير هذا التيقن من سلامة النظام لا يمكن ضمان فعالية أو جدوى أي من الأساليب والممارسات المقصود بها حماية الخصوصية وزيادة الأمان.

هذا الفصل يتناول كيفية استخدام أدوات برمجية مثل **أفاست** و**سيايبوت** و**جدار النار كومودو** لحماية الحاسوب من عدوى البرمجيات الخبيثة ومن خروقات المخترقين. البرمجيات المشروحة في هذا الفصل تعمل على نظام التشغيل ويندوز، وهو بطبيعته الأكثر عرضة لمثل هذه التهديدات، إلا أن كل نظم التشغيل يمكن تأمينها بأساليب مشابهة.

سيناريو تطبيقي

أساني ناشط حقوقي في دولة أفريقية، تساعده ابنته سليمة وابنه موهندو في استخدام الحاسوب، وعند معاينتهما الحاسوب عرضا أن يشرحا له كيفية صيانته والمحافظة على سلامته. أساني متحمس للبرمجيات الحرّة، المجانية مفتوحة المصدر، إلا أنه غير متيقن إن كان هذا هو الخيار الأكثر أمانا، لذا فهو يسأل ابنيه المشورة.

ما يتناوله هذا الفصل

- الأخطار التي تتسبب فيها **البرمجيات الخبيثة** وأثرها على الخصوصية وعلى سلامة البيانات، وكذلك على كفاءة الحاسوب والبرمجيات الأخرى للخصوصية
- كيفية استخدام البرمجيات المزكاة للوقاية من تلك تهديدات
- أهمية تحديث البرمجيات
- ميزات استخدام البرمجيات الحرة عند الإمكان

الفيروسات والديدان وأحصنة طروادة

الفيروسات بُرمجات يمكنها عدوى الحواسيب دون معرفة أو إذن المستخدم، وذلك بطريق نسخ نفسها إلى ملفات برمجيات عائلة أو إلى وسائط مثل الأقراص المرنة والمدمجة وشذرات الذاكرة، وبالتالي تنتقل من نظام إلى آخر بانتقال تلك الملفات والوسائط.

الشائع هو استخدام مصطلح "الفيروسات" كلفظ شامل للدلالة على أنواع مختلفة من البرمجيات الخبيثة تضم الديدان وأحصنة طروادة وغيرها. إلا أن تلك الأنواع في الحقيقة تختلف في كيفية تصميمها وأساليب انتشارها.

الديدان برمجات خبيثة تنتقل تلقائيا من نظام إلى آخر مباشرة باستغلال الثغرات الأمنية في النظم دون حاجة إلى عائلٍ وسيطٍ برمجي ؛ غالبا عبر الشبكات، ويمكنها التهام موارد الشبكة وإبطائها إلى حد التوقف، في محاولة سعيها للانتشار وإيجاد مضيفين جدد تصيبهم.

حصان طروادة، مثلما في الأسطورة الإغريقية، برمجية تبدو ظاهريا بريئة أو مفيدة للمستخدم إلا أنها تحمل في داخلها وظائف تحقق أغراض المتحكم فيها، وعادة ما تنتشر بطريق إقناع المستخدم الغافل بتشغيلها بنفسه لتَزرَع ذاتها في حاسوبه وتسيطر عليه كليا أو جزئيا. تُنكَّر أحصنة طروادة في شكل دعابات برمجية، أو موسيقا أو مقاطع فيديو أو عروضا ذات مشغلات مرفقة بها، كما تشيع في مولدات الأرقام التسلسلية للبرمجيات التجارية المقرصنة، ويتبادلها المستخدمون الغافلون دون أن يعلموا ما تُضمره.

كل البرمجيات الخبيثة قد تسبب أضرارا من قَبِيل تدمير البيانات المحفوظة في النظام المصاب، أو التأثير سلبا على أداء الحواسيب والشبكات. بعض البرمجيات الخبيثة لوجودها أعراض واضحة للمستخدم، إلا أن أغلبها لا تكون أعراضها واضحة من النظرة السطحية مما يُصعِّب اكتشافها على كثير من المستخدمين. بعض البرمجيات الخبيثة تُصمَّم كدعابات أو كبرهان على المهارة التقنية وتحدٍ لمنتجي البرمجيات الكبار، ومع أن بعضها حمل ونشر رسائل سياسية دون الإضرار عمليا بالنظم المصابة، إلا أن بعضها قد استخدم في أعمال إجرامية باستغلال الموارد الحاسوبية والشبكية المملوكة لآخرين لمهاجمة الشبكات وإسقاط المواقع أو كسر كلمات السر لصالح المتحكم فيها.

مضادات الفيروسات

توجد مضادات فيروسات **مجانية** جيدة. وما نعنيه هنا هو برمجيات كاملة الوظائف غير محددة بمدة ولا تجريبية (أو يمكن مد أمد استخدامها بكل وظائفها بإجراء بسيط غير مكلف). من هذه البرمجيات ما تنتجه Avira[١]، وAVG[٢]، وأڤاست[٣] (Avast) الذي نشرح استخدامه ونزكيه لقراء هذا الدليل، واستخدامه للأغراض الشخصية غير التجارية يتطلب إجراء تسجيل كل ١٤ شهرا، إلا أن كلا من التسجيل والتحديث الدوري لتعريفات الفيروسات مجاني.

دليل عملي: ابدأ مع دليل أڤاست

يوجد كذلك مضاد فيروسات **حرّ** – مجاني ومفتوح المصدر – هو ClamWin وهو واجهة تعمل في نظام التشغيل ويندوز لمحرك مضاد الفيروسات الحر ClamAV المنشور برخصة جنو العامة، والذي توجد منه إصدارات لنظم تشغيل عديدة. وبالرغم من افتقاره إلى بعض الوظائف المهم وجودها في مضادات الفيروسات التي يمكن الارتكان إليها، مثل الفحص التلقائي في الخلفية — إلا أن ميزته هي إمكان تشغيله من وسيط تخزين محمول، مثل شذرات يواسبي، وبهذا فهو يفيد عند فحص حاسوب ليست لك صلاحية تنصيب برمجيات فيه، مثلما هو الحال عادة في مقاهي الإنترنت أو حتى حواسيب المدرسة أو العمل.

نصائح لاستخدام مضادات الفيروسات بفاعلية

- لا تُشَغِّل أكثر من مضاد فيروسات واحد في أي وقت في النظام ذاته، إذ قد يبطئ هذا من الحاسوب إلى حد غير منتج.
- استخدم مضاد فيروسات يمكِّنُك من تحديث تعريفات الفيروسات دوريا. أغلب مضادات الفيروسات التجارية التي تأتي منصبة مع الحواسيب الجديدة تتطلب تسجيلها (بمقابل مالي) بعد فترة وإلا فإنها تتوقف عن العمل. البرمجيات المُزكّاة هنا تسمح بالتحديث مجانا طوال مدة استخدامها.
- تأكد من أن مضاد الفيروسات الذي تستخدمه مضبوط بحيث يلتمس تحديثات تعريفات البرمجيات الخبيثة دوريا وينبهك إلى وجودها أو يجلبها تلقائيا ؛ إذ تظهر أنواع جديدة من الفيروسات وباقي البرمجيات الخبيثة باستمرار. أڤاست الذي نزكيه لك والمشروح في هذا الدليل يجلب تلقائيا تحديثات التعريفات عبر الإنترنت دوريا.
- فعِّل وظيفة الفحص الآني في مضاد الفيروسات إن وجدت. تختلف تسميات هذه الوظيفة باختلاف البرمجيات والصانعين، لكنها الوظيفة التي تفحص الملفات في الخلفية تلقائيا عند فتحها دون تدخل من المستخدم، وكذلك البرمجيات عند تشغيلها، وأحيانا تفحص الوسائط المحمولة بمجرد إدخالها في السواقات، كما قد تفحص تدفقات البيانات عبر تطبيقات الشبكة كما يفعل أڤاست وغيره، للسيطرة على العدوى فور اكتشافها ومنع تَفَشِّيها. طالع القسم ١.٢.٣ من دليل استخدام أڤاست للمزيد عن "الفاحص المقيم".
- افحص كل الملفات في حاسوبك مرة واحدة على الأقل عند بدء استخدام مضاد الفيروسات للتيَقُّن من سلامتها. بعد ذلك إن أمَّنتَ كل مداخل النظام، وفعَّلت الفحص المقيم، وفحصت كل ما تُنزِّلُه عبر الشبكة والإنترنت وما تتلقاه عبر البريد، وواظبت على فحص الوسائط المحمولة عند وصلها بالحاسوب، فيمكنك أن تطمئن إلى حدٍّ كبير.

الوقاية من العدوى

- كن حذرا عند فتح مرفقات البريد الإلكتروني، ولا تفتح أية مرفقات تتلقاها ممن لا تعرفهم، وكذلك يفضَّل ألا تفتح مرفقات لم يشرح لك مرسلها طبيعتها أو لم تكن تتوقعها مسبقا كجزء من عملك. وإن أردت فتح مرفقة فعليك حفظها وفحصها أولا، إلا إن كانت وظيفة الفحص الآني مفعَّلة.
- تجنَّب إرسال الملفات التنفيذية كمرفقات، واطلب ممن تراسلهم أن يتجنبوا ذلك إذ لا حاجة له. كما أنه في معظم الحالات لا توجد حاجة لكتابة الرسالة في وثيقة معالج كلمات ثم حفظها وإرسالها كمرفقة بالبريد، بل يُفضَّل كتابة الرسالة في المتن مباشرة وتلافي استخدام المرفقات ؛ وإن اضطررت لإرفاق وثيقة فليكن ذلك في صيغة آمنة مثل rtf.
- قبل وصل وسائط محمولة، مثل الأقراص المرنة أو المدمجة أو شذرات يواسبي تأكد من أن مضاد الفيروسات يعمل وأنه محدَّث، وأن وظيفة الفاحص المقيم تعمل أو افحص الوسيط يدويا.
- الحل الأمثل للوقاية من الفيروسات هو استخدام نظام تشغيل حرٍّ مثل جنو/لينكس.

أساني : لديَّ مضاد فيروسات و أنا أحدثه دوريا، فهل يضمن هذا سلامة حاسوبي ؟

سليمة : الحقيقة أن مضاد الفيروسات وحده لا يكفي، فعليك كذلك حماية الحاسوب من المخترقين و من البرمجيات التجسسية، لذا فسيكون عليك تنصيب و استعمال أداتين أخريتين.

البرمجيات التجسسية

البرمجيات التجسسية فئة من **البرمجيات الخبيثة** تصمم لتنقل إلى من يتحكم فيها بيانات من نظام يخص غيره بلا علم مالك النظام المصاب أو رغبته. يمكن للبرمجيات الخبيثة أن تحفظ مثلا كل ما تدخله باستخدام لوحة المفاتيح، وأسماء التطبيقات التي تستخدمها، ومحتوى الملفات و الوثائق التي تعمل عليها، ومواقع الوب التي تزورها، بل وحتى تصوير ما تراه على الشاشة، وإرسال كل ذلك عبر الشبكة إلى من يتحكم فيها، الذي قد يكون دافعه الفضول، أو غرضا أمنيًا، أو أغراضًا تسويقية تجارية.

قد تكون البرمجيات التجسسية مُتضَمَّنة في أحصنة طروادة، أو قد تنتشر كما تنتشر الفيروسات والديدان، لذا فالوقاية من البرمجيات الخبيثة تلك مهم للغاية. كما أن بعض البرمجيات التجسسية تكون متضمنة في **برمجيات مجانية** أو تجارية تؤدي وظائف مطلوبة، وعادة ما يشكل اكتشافها فضيحة لمنتج البرمجية ومؤذيا لسمعته.

أساني : يبدو هذا كتقنيات جاسوسية في فِلم خيالي ! هل حاسوبي حقا مصاب بكل هذا ؟

موهندو : صدِّق أو لا تصدق ! هذه البرمجيات شائعة بالفعل. إن لم تكن بعض تلك البرمجيات التي تنزَّلها طوال الوقت من الإنترنت لتجربتها قد زرعت بالفعل جواسيس في نظامك فمن الممكن أن تصاب بها عن طريق موقع تزوره يصممه صاحبه لاستغلال بعض الثغرات الأمنية في متصفح الوب. وكونك تستخدم وندوز والإنترنت إكسبلورر يزيد من أرجحية حدوث ذلك. إن لم تكن قد فحصت حاسوبك أبدا فسيدهشك ما ستجده فيه !

صائدات البرمجيات التجسسية

لدرء هذه الأخطار استخدم مضادات البرمجيات الخبيثة. سپايبوت أحد تلك البرمجيات وهو مفيد في الكشف عن البرمجيات الخبيثة المتسللة التي يتجاهلها مضاد الفيروسات. ومثلما هو الحال مع مضاد الفيروسات فمن المهم جدا تحديث تعريفات البرمجيات الخبيثة وإجراء الفحص دوريا.

دليل عملي: ابدأ مع دليل سپايبوت

الوقاية من العدوى

- تنبّه عند تصفح مواقع جديدة، واقرأ الرسائل التي يُظهِرها المتصفح قبل أن تضغط موافق أو نعم، وعندما تشُكُّ فينبغي دوما إغلاق نافذة الحوار بضغط زر × في إطار النافذة لأن هذا يضمن عدم نفاذ أي إجراء قد يكون ضارا.
- زِد من أمان المتصفح بضبطه بحيث لا يُشغِّل تلقائيا البرمجات المُضمَّنة في صفحات المواقع التي تزورها. إن كنت تستخدم **فيرفكس** فيمكنك أن تعطل جافاسكرِبت أو أن تستخدم ملحقة مثل **نوسكربت** لتحكم أدق فيما يشتغل من سكربتات. وإذا كنت تستخدم الإنترنت إكسبلورر فانتقل إلى استخدام فيرفكس أو متصفح آمن غيره.
- في كل الأحوال لا تقبل تنصيب أو تنزيل برمجيات أو ملحقات للمتصفح من مواقع لا تعرفها أو لا تثق بها بما يكفي.

أساني : سمعتُ أن بُرَمِجات جافا و تَحَكُّمات أكتِف‌إكس يمكن أن تكون ضارة، إلا أني لا أعرف ما هي أصلا ؟

سليمة : كلها في النهاية تطبيقات مختلفة لذات الفكرة ؛ فهي بُرمِجات صغيرة تحويها الصفحات وينزلها المتصفح أثناء تصفحك بهدف إضافة وظائف معينة أو عرض أنواع خاصة من المحتوى، والهدف الأصلي منها هو زيادة فائدة المواقع للمستخدمين، إلا أنه بسبب ثغرات أمنية وعيوب في تصميمها وفي المتصفحات فإنه قد يمكن استغلالها لنشر البرمجيات الخبيثة أو الإضرار بنظام المستخدم دون علمه أو رغبته. مقاومة هذه الأخطار تتوزع ما بين مضادات الفيروسات ومضادات البرمجيات التجسسية، كما تعتمد إلى حد كبير على جودة المتصفح وإحكام تحكمات الأمان فيه.

جدران النار

جدار النار هو خط الدفاع الأول الذي تمر عبره تدفقات البيانات القادمة من الشبكة والخارجة إليها، لذا فبالإمكان استخدامه للتحكم في منفذ الحاسوب على الشبكة وتحديد البيانات المسموح لها بالمرور في أي اتجاه وفقا لمعايير متنوعة. من البديهي أن حماية النظام من الاتصالات غير المرغوب فيها الواردة من الشبكة أمر هام لدرء هجمات **المخترقين** و**البرمجيات الخبيثة**، إلا أن مراقبة الاتصالات الصادرة من الحاسوب إلى الشبكة هو كذلك أمر هام للغاية لأنه يكون خط دفاع ثانٍ لمنع البرمجيات الخبيثة التي تسللت إلى النظام من إرسال أي بيانات خاصة جمعتها من النظام إلى خارجه، أو نشر نفسها لعدوى أجهزة أخرى، أو استغلال موارد الشبكة والحاسوب لصالح طرف آخر بأي شكل، وعموما من المهم معرفة البيانات التي تحاول حتى البرمجيات الموثوقة إخراجها من النظام.

جدار النار الجيد يتيح للمستخدم تحديد صلاحيات النفاذ لكل برمجية في الحاسوب، ويطبق تلك القواعد عندما يبدأ أي تطبيق اتصالا عبر الشبكة، أو قد يُضبط لينبه المستخدم لاتخاذ القرار المناسب بالسماح أو المنع.

برمجيات جدران النار

الإصدارات الحديثة من نظام التشغيل ميكروسوفت وِندوز تتضمن جدارا ناريا، إلا أن إمكاناته محدودة مقارنة بغيره كما أن استخدامه ليس يسيرا بالقدر الكافي الذي يجعله مفيدا، لذا فإننا نزكي بديلا **مجانيا** هو جدار النار كومودو[٤].

دليل عملي: ابدأ مع دليل جدار النار كومودو

أسامي : إذن تريداني أن أنصّب في حاسوبي مضادا للفيروسات، ومضادا للبرمجيات التجسسية وجدارا ناريا ! هل سيتحمل حاسوبي كل هذا ؟

موهندو : بالطبع، والحقيقة أن البرمجيات الثلاثة تلك هي الحدُّ الأدنى اللازم للحفاظ على سلامة حاسوب متصل بالإنترنت، ولن يسبب تنصيبها جميعا أية مشكلات في حاسوب متوسط الحداثة. لكن تذكَّر ألا تنصب أكثر من برمجية واحدة من كل نوع في الوقت ذاته، فلا جداران ناريان ولا مضادان للبرمجيات التجسسية ولا الفيروسات.

تأمين المنافذ الشبكية

- لا تنصب في الحاسوب الذي تستخدمه في الأعمال الهامة سوى البرمجيات الضرورية وحسب، وتأكد من أن تجلب تلك البرمجيات التي تنصبها من مصادر موثوق فيها، وأزل كل البرمجيات التي لا تستخدمها.
- افصل حاسوبك عن الإنترنت ما لم تكن في حاجة إليها، وأطفئ الحاسوب تماما أثناء الليل، ما لم تكن قد ضبطته ليؤدي عملا ما في ذلك الوقت استثناءً.
- لا تُعطِ كلمة سر حسابك في نظام التشغيل لأي شخص، وإن كان آخرون يستخدمون الحاسوب معك فأنشئ لكل مستخدمٍ حسابًا منفصلا ؛ هذا يَسير جدًا في كل نظم التشغيل بما فيها وِندوز.
- عطِّل **خدمات وِندوز** التي لا تستخدمها وغير الضرورية لعملك. استعن بمن لديه خبرة تقنية إن لزم الأمر.
- تأكد من تنصيب جدران نارية على كل الحواسيب في شبكة المكتب، وكذلك تحقق من إعدادات الجدار الناري في الجهاز الذي تستخدمه لوصل الإنترنت بشبكة المكتب أو المنزل، سواء كان مودما أو مسيرا أو مزيجا منهما في جهاز واحد.

البرمجيات الحرة

البرمجيات التجارية – المحمية حقوق طبعها – عادة ما يتطلب تنصيبها واستخدامها في وقتنا الحاضر إثبات أصالة النسخة وسداد ثمنها، وعادة ما يكون الإثبات في شكل رقم تسلسلي فريد أو مفتاحا رقميا، كما يتطلب بعضها تفعيلا بالاتصال بموقع الصانع عبر الإنترنت. البرمجيات المنسوخة أو المقرصنة قد تعطل بعضا من وظائفها أو كلها، ونظام التشغيل وِندوز سيمتنع عن تحديث مكوناته

عبر الإنترنت إن كانت النسخة العاملة مقرصنة أو مسروقة، وهذا قد يترك حاسوبك وبياناتك عرضة للمخاطر، كما قد يتسبب في تعطيل عملك بشكل مفاجئ في أوقات حرجة إن توقفت البرمجيات عن العمل فجأة.

استخدام البرمجيات المقرصنة مُجرَّمٌ قانونا في معظم القضاءات، وقد يعرض منظمتك إلى مخاطر قانونية تتراوح ما بين الغرامات ومصادرة العتاد وصولا إلى سحب تراخيص المؤسسات وإغلاقها، وهو مبرر قانوني تسهل على السلطات إساءة استغلاله في الدول التي توجد فيها سياسات وتوجهات معادية لمنظمات المجتمع المدني، أو تلك العاملة في مجال معين.

لحسن الحظ، يوجد بديل يغنيك عن إنفاق أموال طائلة على البرمجيات، وهي **البرمجيات المجانية** و**البرمجيات الحرة**، التي تتوافر فيها بدائل لكل البرمجيات التجارية التي تحتاجها، وخصوصا تلك التي ليست لديك تراخيص لها.

البرمجيات الحُرَّة يصممها ويؤلفها أفراد ومنظمات من مختلف البلاد والمشارب، وبعضها مشاريع تعاونية يشترك فيها آلاف الأفراد وتقدر القيمة الكلية لبعضها بمليارات الدولارات، والمقارنة بينها بين البرمجيات التجارية من حيث الجودة غير ذات بال، كما أن شركات البرمجيات التجارية أحيانا ما تستفيد منها في أعمالها أو تنشر بعض إنتاجها برخص حرّة.

الرأي السائد حاليا – وله معارضون بالطبع – هو أن البرمجيات الحرّة، لأنها مفتوحة المصدر، أكثر أمنا من البرمجيات التجارية، وذلك لأنها تطور بشفافية ويمكن لأعداد أكبر ممن لديهم الخبرة التقنية الاطلاع على **أكوادها المصدرية** وبالتالي اكتشاف العلات بشكل أكثر كفاءة. و**فيما يتعلق بالسرية والخصوصية بالذات فإن الخبراء ينصحون بعدم الوثوق سوى في البرمجيات التي يمكن الاطلاع على شفرتها المصدرية**.

توجد برمجيات حرة عديدة مكتوبة خصيصا لنظام التشغيل وِندوز، ويمكنك أن تستكشف البدائل الحرة المتاحة في أحد التطبيقات، مثل مستعرضات الإنترنت، أو حزم البرامج المكتبية، وأن تستخدمها جنبا إلى جنب مع البرمجيات التي اعتدتها حتى تعتاد البرمجيات الحرة وتتيقن من أنها تغطي كل حاجاتك، واعلم أن البرمجيات الحرة بوسعها أن تنتج وتقرأ وتعالج وثائق الملفات في الصيغ الشائعة، لذا فسيظل بوسعك العمل مع زملاء لا يستخدمون ذات البرمجيات والأدوات التي تستخدمها.

بعد أن تطمئن إلى جودة البرمجيات الحرة التي اخترتها من البدائل العديدة المتاحة، وإلى أنها تؤدي كل الوظائف التي تحتاجها لأداء عملك يمكنك الانتقال من نظم التشغيل التجارية/المقرصنة إلى نظام تشغيل حرٍّ، مثل جنو/لينكس في أحد توزيعاته العديدة ؛ بل يمكنك تجربة نظام تشغيل حرٍّ دون تغيير إعدادات حاسوبك أو العبث بتهيئة الأقراص أو خشية فقد البيانات والتضبيطات الحالية، وذلك بطريق تنزيل صورة **قرص حي** لإحدى التوزيعات الشائعة[٥] مثل أوبونتو أو طلبها بالبريد وتجربتها بعد تسجيلها على قرص مدمج بوضعه في المشغل والإقلاع منه. وعند الفراغ من التجربة يمكنك إعادة تشغيل الحاسوب لتجد أن كل شيء في نظامك الحالي لم يتغير.

تحديث البرمجيات

البرمجيات إبداعات هندسية كبيرة ومعقدة، ومن المحتوم أن تطرأ في بعض مكوناتها المتداخلة ومراحل تصميمها وتنفيذها العديدة أعطال وعيوب في التصميم، ومن البدهي أن بعض تلك

العلات قد يؤثر سلبا على أمن الحواسيب والنظم التي تستخدمها أو توجد ثغرات أمنية يمكن استغلالها، بدرجات متفاوتة من الخطورة. ينطبق هذا على البرمجيات التجارية من أكبر الشركات كما ينطبق على البرمجيات الحرة وعلى المجانية.

يعمل مطورو البرمجيات على الكشف عن تلك العيوب وإصلاحها وتحسين التصميمات باستمرار في إصدارات متعاقبة، لذا فمن الضروري أن تُحدِّث دوريا البرمجيات التي تستخدمها، بما فيها نظام التشغيل، ومن المحبذ أن تطلِّع على تأريخ كل إصدارة حديثة قبل تنصيبها للوقوف على العلات التي عولجت والعيوب المعروفة فيها، والوظائف التي أضيف أو أزيلت.

نظم التشغيل الحديثة توجد بها وظائف لالتماس وتنزيل وتنصيب تحديثات مكوناتها تلقائيا عبر الشبكة. في وِندوز تسمى تلك الوظيفة التحديث التلقائي Auto Update.

روابط إلى الوب

[١] http://www.avira.com
[٢] http://free.avg.com
[٣] http://ar.security.ngoinabox.org/avast
[٤] http://ar.security.ngoinabox.org/comodofirewall
[٥] http://www.ubuntu.com

٢
الحماية من الأخطار الماديّة

٢. الحماية من الأخطار الماديّة

مهما بلغ الجهد الذي تبذله في تصميم الدفاعات الرقمية حول نظامك وبياناتك فمن الممكن أن تصحو يوما لتجد الحاسوب قد فقد، سُرق أو صودر أو أُعطب، عمدا أو عرضا، أو أن البيانات التي عليه قد تَلِفت أو نُسخت، فعوامل مثل تذبذب التيار الكهربي، وانسكاب أكواب المشروبات، والنوافذ أو الأبواب غير المحكمة كلها يمكن أن تتسبب في النهاية في ضياع البيانات وعدم القدرة على استخدام الحاسوب. يفيد التحليل المتأني للمخاطر المحتملة في إيجاد بيئة مواتية للعمل وتطوير **سياسة أمان** لتلافي آثار مثل تلك الأحداث.

سيناريو تطبيقي

شِنجاي ورودو زوجان مسنان لديهما خبرة طويلة في مجال مساعدة المصابين بالإيدز في زمبابوي على الحصول على العلاجات اللازمة، وقد تقدما بطلب منحة لشراء حاسوب وعتاد شبكة لمكتبهما. وحيث إنهما يعيشان في إقليم تغشاه الاضطرابات من حين لآخر، سياسيا ومن ناحية البنية التحتية، فإنهما وممولهما يرغبون في التأكد من أن الحاسوب المُشترى سيكون بمأمن، ليس فقط فيما يتعلق بالفيروسات والمخترقين، بل كذلك من السرقة والمصادرة وصواعق البرق والكوارث الأخرى. لذا فقد سألا أوتو، وهو فني حواسيب، أن يساعدهما في وضع خطة لتحسين الأمان المادي للحاسوب وعتاد الشبكة التي ينويان شراءها إن قُبل طلبهما للمنحة.

ما يتناوله هذا الفصل

- **الأخطار المادية** التي تهدد الحاسوب والمعلومات المخزنة فيه
- سبل تأمين العتاد الحاسوبيّ من تلك المخاطر
- مقومات إيجاد بيئة آمنة لتشغيل الحواسيب والشبكات
- الاعتبارات الواجب أخذها في الحسبان عند وضع سياسة تأمين للحواسيب في مقر العمل

تقييم المخاطر

تُقلل منظمات عديدة من أهمية التأمين المادي لمكاتبها وعتادها، ونتيجة لذلك فهم يفتقرون غالبا إلى سياسة واضحة تبين ما الذي ينبغي عليهم فعله لحماية حواسيبهم ووسائط تخزينهم من السرقة، وعوامل المناخ، والحوادث وتهديدات مادية أخرى. قد تكون أهمية تلك السياسات بادية إلا أن تطويرها أصعب مما يبدو للوهلة الأولى. فمثلا، لدى كثير من المنظمات أقفال متينة على أبواب مكاتبها وقد تكون لديها نوافذ مصفحة، لكنهم إن لم ينتبهوا إلى عدد المفاتيح التي صنعت لتلك الأقفال ومن لديه نسخ منها فإن بياناتهم تظل مهددة.

شِنجاي : نود وضع ملخص لسياسة التأمين في طلب المنحة، إلا أننا نريد التيقن من أن السياسة ذاتها شاملة. ما الذي ينبغي تضمينه فيها ؟

أوتو : أخشى أنه لا يوجد حل مسبق الإعداد لمواجهة التهديدات المادية، فوضع سياسة جيدة يجب أن يستند إلى ظروف كل منظمة. لكن هاك نصيحة عامة : عندما تسعى لوضع سياسة ينبغي لك ملاحظة بيئة العمل بتمعن واكتشاف مواطن الضعف وكيفية تدعيمها.

عند تقييم المخاطر ومواطن الضعف التي تواجهها المنظمة ينبغي تقييم عدة مستويات يمكن أن تكون فيها تهديدات للبيانات :

- قنوات الاتصال المستخدمة وكيفية استخدامها. أمثلة ذلك تشمل البريد التقليدي، والفاكسات، وخطوط الهاتف الأرضي والمحمول، والبريد الإلكتروني، والمحادثات عبر الإنترنت.
- كيفية تخزين البيانات المهمة. الحواسيب وسواقات الأقراص، والبريد الإلكتروني وخواديم الوب وذرات ذاكرة يوإسبي والسواقات المحمولة والخارجية وأقراص الليزر المدمجة والهواتف المحمولة والكاميرات ومسجلات الصوت والأوراق المطبوعة والملحوظات اليدوية والمسودات، كلها مواطن ضعف محتمل.
- أماكن حفظ حاويات المعلومات تلك. قد يكون هذا في المكتب، أو في البيت، أو في صندوق المهملات في الخارج، أو في موضع ما على الإنترنت، وفي الحالة الأخيرة قد يكون من العسير تعيين الموضع المادي للمعلومات.

راعِ أن المعلومة ذاتها قد يتهددها أكثر من تهديد في مستويات مختلفة. كذلك لاحظ أن بعض الممارسات قد تفيد في مواجهة التحديات الرقمية والمادية، مثل الحفظ الاحتياطي في مكان آمن الذي قد يفيد في حالة الكوارث وكذلك للحماية من المخاطر الرقمية كالڤيروسات، إلا أن بعض الممارسات لا تفيد سوى في نطاق معين.

عندما تُفاضِلُ ما بين أن تضع شريحة يوإسبي في جيبك أو في قعر حقيبتك داخل كيس بلاستيكي محكم فإنك تتخذ قرارات تتعلق بالأمان المادي، بالرغم من أن البيانات التي تسعى لحمايتها رقمية. هل يحتمل أن تترك غيرك يحمل حقيبتك في أي وقت ؟ هل يحتمل أن يفتشها أحد ؟ هذه هي نوعية الأسئلة التي ينبغي التفكير فيها عند اتخاذ قرار كهذا.

حماية البيانات من الاختراق المادي

يشكل أولئك الذين يريدون الحصول على معلومات تخصك فئة هامة من **التهديدات المادية**، ومثلما هو من الخطأ الظن بأن هذا هو الخطر الوحيد الذي يتهدد بياناتك، فإنه من الخطأ تجاهل هذا الخطر.

توجد عدة إجراءات يمكن باتباعها تقليل خطر الاختراق المادي. التصنيفات والاقتراحات التالية، والتي ينطبق معظمها على المنزل كما على المكتب، تشكل أساسا يمكن البناء عليه بما يتناسب والتهديدات المحددة التي تواجهك.

في محيط المكتب

- اعرف جيرانك. فبناء على مناخ الأمان في بلدك وحيّك، يمكن أن ينتج أحد وضعين : إما أن يصبح جيرانك حلفاء لك يحرسون مكتبك، أو أن ينضموا إلى قائمة أعدائك الواجب الحذر منهم.
- راجع كيفية تأمين كل الأبواب والنوافذ والمداخل الأخرى التي تؤدي إلى المكتب.
- فكّر في إمكانية وضع كامرا مراقبة أو متحسسا للحركة متصلا بجرس إنذار.
- حاول إنشاء منطقة استقبال يلتقي فيها العاملون بالزوار قبل أن يدلفوا إلى المكتب، وكذلك غرفة اجتماعات منفصلة عن منطقة العمل.

داخل المكتب

- احم كوابل شبكة الحاسوب بأن تمررها داخل المكتب وليس على الجدران الخارجية ؛ يفضل كذلك ضبط إعدادات الشبكة بحيث تستخدم الحواسيب بروتوكولات التعمية IPSec لدى الاتصال فيما بينها.
- ضع الأجهزة الشبكية مثل **الخواديم** و**المُسيِّرات** والبدالات (الحاسوبية والهاتفية) و**المودمات** في غرف أو خِزانات مؤمّنة. المخترق الذي يمكنه الوصول إلى تلك الأجهزة سيكون بوسعه زرع أجهزة تنصت أو **برمجيات خبيثة** يمكنها نقل البيانات إليه أو تمكنه من اختراق مزيد من الحواسيب حتى بعد مغادرته.
- إن كانت لديك شبكة حاسوبية لاسلكية فمن المهم ضبط **نقطة الاتصال اللاسلكي** لتأمينها بحيث لا يمكن لأيٍ كان الاتصال بها والنفاذ إلى الشبكة المحلية أو مراقبة تدفقات البيانات. ابحث في إعدادات الجهاز عن خيارات التعمية، مثل WPA أو WEP الأضعف وفعِّلها، وغير كلمة السر كل فترة معقولة، أسبوعيا أو شهريا ؛ وإن كانت الحواسيب التي تتصل بالشبكة محددة مسبقا ولا تتغير كثيرا مسبقا فيمكن ضبط نقطة الاتصال اللاسلكي بحيث لا تقبل اتصالات سوى من الأجهزة ذوات **عناوين التحكم في النفاذ للوسيط** (MAC address) التي في قائمة حصرية. لاحظ أنه في حالة الشبكات اللاسلكية فإن أي شخص في محيط يسمح له بالتقاط الإشارة اللاسلكية يمكن أن يكون مقتحما.

في مكان العمل

- يجب أن توجه شاشات الحواسيب بعناية، بحيث تصعب على المارّين ملاحظة المعروض عليها من بيانات، في المكتب قد يعني هذا أن تؤخذ في الحسبان مواضع النوافذ والأبواب ومكان استقبال الزوار.
- في معظم صناديق الحواسيب توجد فتحة يمكن فيها تمرير أقفال تمنع فتحها، وذلك لمنع العبث بمكوناتها الداخلية، يمكنك أن تضيف هذه الخصيصة على قائمة ما تتحقق منه عند شراء حواسيب جديدة.
- استخدم سلاسل الأمان إن أمكن لمنع غير المصرح لهم من نقل الحواسيب من مواضعها أو سرقتها، هذا هام في حالة الحواسيب الصغيرة التي يمكن حملها وإخفاؤها بسهولة.

برمجيات و تضبيطات ذات علاقة بالتأمين المادي

- تأكد من أن حاسوبك يتطلب كلمة سر عند تشغيله قبل أن يسمح لك بالنفاذ إلى البيانات المخزنة فيه أو تنصيب برمجيات أو استخدامه عموما بأي شكل. في وندوز يمكن تفعيل هذه الوظيفة من لوحة التحكم في تحكمات المستخدمين، حيث تختر تضبيطات حسابك و تفعِّل كلمة السرِّ. ضع كلمة سر قوية كما هو موصوف في فصل ٣: "وضع كلمات سرٍّ قوية و حفظها".
- توجد إعدادات في **بيوس** الحاسوب (BIOS) تخص التأمين الماديّ، منها ضبط الحاسوب بحيث لا يقلع من سَوّاقات الأقراص المدمجة أو الأقراص المرنة أو ذواكر يوإس‌بي أو الشبكة (إن كنت لا تستخدمها)، والهدف من هذا منع تشغيل برمجيات تسيطر على الحاسوب أو تخترقه قبل أن تتاح الفرصة لنظام التشغيل لتطبيق سياسات الأمان المحددة له. تَذَكَّر بعد أن تعطل الإقلاع من المشغلات الخارجية أن تضع كلمة سر قوية على إعدادات بيوس بحيث لا يمكن لآخرين تغييرها.
- إن كنت تستخدم أداة لإدارة كلمات السر أو تحفظها كما هو مشروح في الفصل المشار إليه عاليه فتَذَكَّر ألا تكون نسختك الوحيدة من الملف الحاوي كلمات السر محفوظة على الحاسوب ولا غيرها.
- اعتد أن تقفل حسابك على الحاسوب كلما نويت الابتعاد عنه لفترة ولو قصيرة. يمكن فعل هذا في ويندوز بسرعة بضغط زر أيقونة النوافذ في لوحة المفاتيح مع حرف L ؛ إلا أن هذا لن يعمل إلا إن كنت وضعت كلمة سر على الحساب كما هو مشروح عاليه
- **عمّ** البيانات الحساسة المخزنة في الحاسوب ووسائط التخزين الأخرى في المكتب. طالع فصل ٤: "حفظ سرية البيانات الحساسة" لمزيد من التفاصيل عن هذا الموضوع وإحالات إلى الأدوات المطلوبة.

رودو : أنا أخشى العبث في تضبطيات بيوس الحاسوب، لأني أخشى أن أخرب شيئا لا أعرف كيفية إصلاحه، فهل هذا ممكن ؟

أوتو : إن حدث هذا فلن يكون عطلا دائما، والحقيقة أن التحكمات المطلوب ضبطها بسيطة جدا، إلا أن واجهة التحكم ذاتها قد تكون هي ما يُحدث الرهبة. قد يؤدي خطأ ما إلى أن يتعذّر إقلاع الحاسوب، لكن لا شيء خطر أو لا يمكن إصلاحه، عموما يمكنك الاستعانة بخبير.

الأجهزة المحمولة

- لا تَغفل أبدا عن حاسوبك المحمول أو الهاتف المحمول أو الأجهزة الأخرى التي تحوي بيانات حساسة، خاصة إن كنت مسافرا أو تقيم في فندق أو تجلس في مكان عام. استخدام سلسلة أمان قد يكون فكرة جيدة، إلا أنه أحيانا ما يصعب إيجاد شيء ملائم لربط الحاسوب إليه. تذَكَّر أن أوقات تناول الوجبات عادة ما يستغلها اللصوص الذين تعلَّم كثيرون منهم اقتحام غرف الفنادق في الأوقات التي لا يحتمل أن تكون مشغولة فيها.

- إن كان لديك حاسوب محمول أو أداة حاسوبية يدوية فتفادى وضعها أو تعليقها بحيث تلفت الأنظار، فلا حاجة لتنبيه اللصوص أن معك ما يستحق السرقة، ولا إعلام من قد يريد سرقة بيانات منك أن حقيبة يدك أو ظهرك فيها سواقة صلبة مليئة بالمعلومات. أحيانا قد يكون من الحكمة تفادي استخدام الأجهزة المحمولة في الأماكن العامة، وحمل الحاسوب في حقيبة لا تبدو أنها حقيبة حاسوب.

إيجاد بيئة ملائمة للعتاد الحاسوبي

مثل كثير من الأجهزة الإلكترونية فإن الحواسيب بالغة الحساسية، فهي لا تتوافق جيدا مع التذبذبات في التيار الكهربي، ولا درجات الحرارة المتطرفة، ولا الغبار ولا الرطوبة العالية أو الإجهاد الميكانيكي. لحماية حاسوبك وعتادك الشبكي من تلك المخاطر اتَّبع التالي :

- المشكلات الكهربية مثل تذبذب التيار، وانقطاعات الطاقة يمكن أن تتلف الحاسوب ماديا، فهذه التذبذبات يمكنها أن تخرب سواقة القرص الصلب متلفة البيانات المحفوظة عليه، أو تضر المكونات الإلكترونية في الحاسوب.
  - استخدم **مصادر التيار غير المنقطع** (UPS: unintteruptable power supply) إن كان بمقدروك شراؤها.
  - إن كان استخدام مصادر التيار غير المنقطع غير ملائم أو مكلفا فاستخدم مثبتات التيار لحماية الحواسيب، فهي أقل كلفة لكنها توفر حماية جيدة من تذبذبات التيار.
  - اختبر الشبكة الكهربية قبل إيصال أجهزة ثمينة إليها، يفضل استخدام مقابس الكهرباء ذات الأطراف الثلاثة أينما وجدت لأن الطرف الأرضي يساعد على حماية الأجهزة. وإن أمكن فاقضِ يومين في مراقبة كفاءة الشبكة الكهربية في مقر جديد أو منزل جديد وأثرها على المصابيح والمراوح قبل إيصال الأجهزة الإلكترونية الثمينة بها.
- للوقاية من الحوادث عموما تجنّب وضع الأجهزة الهامة في الممرات، أو منطقة الاستقبال والمواضع الأخرى غير المحمية، مقابس الكهرباء ومثبتات التيار ومصادر التيار غير المنقطع وتطويلات الوصلات الكهربية الموصولة بالخواديم وأجهزة الشبكة يجب أن توضع بحيث لا يكون من المحتمل إطفاؤها بطريق الخطأ أو العبث.
- إن كان بإمكانك شراء كوابل حواسيب وتطويلات كهربية عالية الجودة فينبغي شراء ما يكفي منها لتغطية احتياجات المكتب كله وزيادة للاحتياط ؛ فالمقابس غير المحكمة التي تنفصل بسهولة أو تهتز وتصدر شررا ليست مزعجة وحسب بل قد تتلف الأجهزة المتصلة بها كما قد تشعل حرائق، خاصة إذا ما عمد الأشخاص المُحنَقون إلى تثبيت المقابس بأشرطة لاصقة من مواد ملتهبة !
- إن كنت تحفظ أيا من الحواسيب في خِزانات فتأكد من أنها جيدة التهوية وإلا فقد تسخن.
- لا يجب وضع الحواسيب قرب المدافئ والمشعات أو أجهزة التكييف أو غيرها من مسارب.

شِنجاي : الحقيقة أننا قد تغلبنا للتو على بعض من تلك المشكلات سابقا هذا العام، وقد أمضينا شهورا نبحث عن كوابل محكمة لا تسقط من مقابس الحواسيب.

أوتو : و مقابس مشتركة لا تنذر بإشعال السجاد ؟

شِنجاي : و هذه أيضا. في النهاية اضطر رودو إلى جلب بعضها معه من يوهانسبرج. مع هذا فلا يزال التيار الكهربي غير مستقر، إلا أن الأجهزة أصبحت أكثر استقرارا على الأقل.

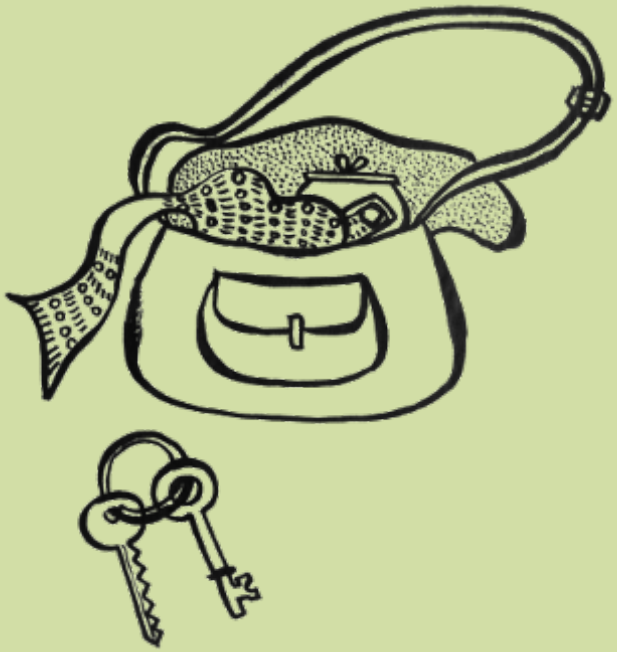
وضع سياسة التأمين المادي

بعد أن تقيِّم المخاطر ومواطن الضعف التي تواجهها المنظمة عليك التفكير في الخطوات التي سيحسن اتخاذها من الأمان المادي. ينبغي وضع سياسة أمان تفصيلية مكتوبة. الوثيقة الناتجة ستكون بمثابة إطار دالٍّ لك ولزملائك وللقادمين الجدد إلى المنظمة. ينبغي أن تضم الوثيقة قائمة بالإجراءات الواجب اتِّباعها في حال تحقق كل من المخاطر المذكورة. كل المعنيين ينبغي أن يقرأوا الوثيقة ويفهموها ويطبقوها عند الحاجة. كما ينبغي تشجيع الأسئلة والاقتراحات لتحسين الوثيقة باستمرار. قد تحوي سياسة الأمان المادي بعض أو كل التالي، حسب الظروف :

- سياسة استخدام المكتب، تتضمن أجهزة الإنذار والمفاتيح، ومن يسمح له بالتواجد في المكتب ومن المسؤول عن خدمة النظافة، وما شابه.
- سياسة تحديد مناطق المكتب المحظور على الزوار التواجد فيها.
- حصرا بالمعدات والأجهزة بما فيها الأرقام المتسلسلة والأوصاف المادية.
- خطة للتخلص الآمن من الأوراق المستهلكة التي قد تحوي بيانات حسَاسة.
- إجراءات طوارئ للحالات التالية :
  - من ينبغي إخطاره فور اكتشاف تسرب بيانات حسّاسة.
  - من ينبغي الاتصال بهم في حال وقوع حريق أو فيضان أو كارثة طبيعية أخرى.
  - كيفية الاتصال بشركات المرافق، مثل الكهرباء والماء والإنترنت.
  - كيفية استرجاع المعلومات من المحفوظات الاحتياطية التي خارج المقرِّ. يوجد مزيد من المعلومات عن الحفظ الاحتياطي في فصل ٥: "تدارك فقد البيانات".

يجب مراجعة **سياسة** الأمان دوريا وتحديثها لتعكس التغيرات في السياسات والإجراءات والمعلومات التي طرأت منذ آخر مراجعة، وبالطبع لا تنس حفظ وثيقة سياسة الأمان مع الوثائق الهامة.

٣
وضع كلمات سر قوية وحفظها



٣. وضع كلمات سر قوية وحفظها

تتطلب كثير من الأساليب التقنية التي نعتمد عليها لزيادة أمان تقنيات المعلوماتية التي نستخدمها، من الولوج إلى حساباتنا على الحواسيب أو في مواضع الخدمات المختلفة، إلى **تعمية** البيانات السرية، تتطلب استخدام كلمة سرّ. كلمات السر أو عبارات السر تلك هي كل ما تتوقف عليه حماية المعلومات وهي ما يحول دون أن يحوزها من لا نرغب. لذا فكثير من أساليب الاختراق يكون محورها هو معرفة كلمات السرّ ؛ وتتراوح ما بين تخمينها، إلى خداعك لإدخالها في المكان غير المناسب، إلى التجسس عليك أثناء إدخالها، وصولا إلى تهديدك لإجبارك للإفصاح عنها.

سيناريو تطبيقي

منصور وماجدة شقيقان من بلد عربي لديهما مدونة ينشران فيها – دون إفصاح عن هويتهما – عن انتهاكات حقوق الإنسان ويحرضان على التغيير السياسي. حاولت ماجدة مؤخرا أن تَلِج إلى حسابها البريدي على الوب فاكتشفت أن كلمة سرها قد تغيَّرت. بعد أن صَفَّرت كلمة السِّر باتباع الإجراء الذي حدده مقدم الخدمة كان بوسعها الولوج مجددا إلى الحساب إلا أنها لاحظت أن عددا من الرسائل التي لم تكن قد رأتها من قبل مؤشر عليها أنها قُرِئَت. لذا فهي تَشُكُّ الآن في أن أحدا قد كشف كلمة سرها واستخدمها لاختراق حسابها بدوافع أمنية سياسية، ولأنها تستخدم كلمة السِّر ذاتها لحساباتها في مواقع وخدمات عديدة، فقد رأت أن تتحدث في الموضوع مع منصور الذي يقل عنها خبرة في مسائل الحواسيب لتوضح له الأمر وتتناقش معه في مخاوفها.

ما يتناوله هذا الفصل

- مقومات كلمة السر القوية
- حيل تساعد على تذكر كلمات سر معقدة
- كيفية استخدام خزانة كلمات السر الآمنة كِيپاس لحفظ كلمات السر بدلا من استظهارها

تأليف كلمات السر القوية والحفاظ عليها

عندما نرغب في حماية شيء منقول فإننا نقفله بمفتاح. المنازل والخزانات والدراجات والسيارات كلها لها مفاتيح وأقفال. للملفات مفاتيح **تعمية**، بطاقات الصراف الآلي لها أرقام تعريف شخصية ولحسابات البريد كلمات سرّ. كل تلك المفاتيح، سواء كانت مادية أو رقمية، تشترك في أنها تفتح أقفالها سواء بيدك أو بيد غيرك. في مجال الحماية الرقمية يمكنك أن تعمي ملفاتك وتضع كلمات سر على الولوج إلى الحسابات، لكن إن انكشفت كلمة السر لغيرك، سواء لأنها ضعيفة أو سهلة التخمين فلن تكون لها فائدة.

مقومات كلمة السر القوية المفيدة

باختصار، ينبغي أن تكون كلمة السر عسيرة على التخمين حتى على من يعرفونك شخصيا، وأن يتطلب استنتاجها حاسوبيا فترة طويلة. لاحظ أنه لو كان لدى مهاجم وقت كاف وقدرات حاسوبية

كافية فالمسألة تتلخص في كونها مسألة وقت قبل أن يتمكن من كسر المفتاح أو استنتاج كلمة السر بتجربة كل التباديل المتاحة. المطلوب هو تصعيب ذلك بقدر الإمكان بما يتلاءم مع قدر سرية البيانات ومدى عزم المهاجم على نيلها.

- **كلما طالت كان أفضل :** بزيادة طول كلمة السر يزيد أسيًّا عدد التوافيق المطلوب من برمجية المهاجم تجربتها. طول كلمة السر يحدده عدد خانات المحارف المستخدمة فيها. عموما ينبغي أن لا يقل طول كلمة السر عن ثمانية محارف، وضعف ذلك لكلمات مفاتيح التعمية (المزيد عن تعمية الملفات في فصل ٤: "حفظ سرية البيانات الحساسة"). كثيرون يضعون كلمات سرٍّ تتألف من أكثر من كلمة بينها مسافات أو لا، وهذه تسمى عبارات المرور، وهي محبذة ما دامت الخدمة أو البرمجية تتقبلها.
- **كلما تعقدت كان أفضل :** إضافة إلى الطول فإن التعقيد يزيد من صعوبة هجومات القوة الغاشمة التي تستخدم فيها الحواسيب – التي لا تكل ولا تمل – في محاولة اكتشاف التوفيقة الصحيحة من المحارف التي تتألف منها كلمة السر. ينبغي بقدر الإمكان أن تتألف كلمة السر من أحرف، وأرقام وعلامات ترقيم ورموز. باختصار استخدم كل الرموز المتاح إدخالها من لوحة المفاتيح، وتذكر أن الأبجدية اللاتينية بها شكلان من كل حرف، كبير وصغير، كما يمكنك استخدام المحارف العربية إلى جانب اللاتينية ما دام النظام يسمح، وما دمت متيقنا من أنه سيكون بوسعك إدخالها كلما احتجتها (ضع في الحسبان اختلاف لوحات المفاتيح في البلدان المختلفة). كثير من التطبيقات التي تعتمد كلمة السر وكذلك الخدمات على الإنترنت التي تتطلب وضع كلمات سر تكون بها مؤشرات لقياس مدى قوة كلمة السر التي تدخلها عندما تفتح الحساب أو تغيِّر كلمة السر القديمة بأخرى جديدة. استرشد بتلك المؤشرات إضافة إلى ما سبق.
- **أن تكون عملية :** "العملانية" معيار نسبي يختلف من شخص لآخر. لكنك إن احتجت إلى كتابة كلمة السر في ورقة لأنك لا تستطيع تذكُّرها فإن ذلك قد يقلل كثيرا من درجة الأمان ويفتح الباب لتهديدات جديدة يمكن أن يستغلها كل من يستطيع أن ينفذ إلى مكتبك أو محفظتك أو حتى سلة المهملات. قسم "تذكر وحفظ كلمات السر" يحوي نصائح قد تساعدك. إن ظلت تلك الأساليب صعبة عليك فربما أمكنك استخدام خِزانة كلمات سرٍّ مثل كِيپاس. لاحظ أن أنواع الملفات الأخرى لا يمكن الاعتماد عليها في غرض حفظ كلمات السر، حتى لو كانت الملفات محمية بكلمات سر، مثل وثائق ميكروسوفت ورد وإكسل، لأن التعمية المستخدمة فيها ضعيفة وتوجد على الإنترنت أدوات يمكنها كسر كلمات سر كثير منها في ثوان.
- **أن تكون غير شخصية :** يجب ألا تكون كلمة السر من المعلومات الشخصية المرتبطة بك، سواء بهويتك الحقيقية أو بالهويات الرقمية التي تستخدمها. فلا تضع كلمات سر تتألف كلها أو جزءا منها من بيانات كاسمك أو اسم زوجتك أو صديقك المقرب، ولا رقم بطاقة هويتك المدنية، ولا رقم هاتفك، ولا اسم ابنتك ولا تاريخ ميلاد ابنك، ولا حتى اسم حيوان كقطتك أو كلبك ؛ فكل هذه المعلومات يمكن معرفتها وجمعها بقليل من البحث.
- **أن تكون سرية :** ربما كان بديهيا وجوب كون كلمة السر سرية، إلا أن الواقع أن كثيرين يشركون الآخرين في كلمات سرِّهم، لأغراض عديدة مثل مساعدتهم على أداء الأعمال، أو حل المشكلات

التقنية، أو مساعدتهم في الحصول على بيانات تهمهم. الأفضل أن تبحث عن وسائل أخرى لمشاركة الآخرين في المعلومات التي تهمهم، وإن اضطررت للإفصاح عن كلمة السر لأحدٍ ليساعدك على حل مشكلة تقنية فينبغي عليك أن تغيِّرها قبل أن تعطيها له وأن تضع مكانها كلمة سر مؤقتة لا تستخدم فيها ذات التكنيكات العقلية التي تستخدمها في تأليف كلمات السرِّ الحقيقية ثم أن تغيِّرها مرة أخرى بعد أن تنتهي المسألة. ينبغي أن تفعل الشيء ذاته إن اخترت أن تدخل كلمة سر إحدى الخدمات على الإنترنت في خدمة أخرى تقترح عليك فعل ذلك لأجل استيراد بياناتك من الخدمة الأولى، وهو ما أصبح شائعا الآن في عديد من الشبكات الاجتماعية وغيرها التي تطلب الولوج إلى بريدك لجلب قائمة معارفك. وتذكّر أن مدير النظام أو مقدم الدَّعم التقني في أي شبكة أو خدمة، سواء على الإنترنت أو في المكتب أو الجامعة، لا يحتاج إلى معرفة كلمة سرّك ليساعدك في حل مشكلة أو أداء عمل. الحفاظ على سرية كلمة السر يتضمن أيضا الحذر ممن قد ينظر من وراء ظهرك أثناء إدخالها.

- **أن تكون فريدة :** تجنب استخدام كلمة السر ذاتها لعديد من الحسابات، وإلا فإن من يكشفها سيكون من السهل عليه النفاذ إلى كم كبير من المعلومات السرية، أو تخريبها، أو حتى انتحال شخصيتك الرقمية. هذا مهم للغاية فيما يتعلق بحسابات البريد الإلكتروني، لأن خدمات عديدة تتيح إجراءات لاستعادة كلمة السر التي تخصها بطريق البريد. كما أن الأمر عموما هام لأن بعض الخدمات والتطبيقات لا تحمي كلمة السر بدرجة كافية، مما يسهل اكتشافها، وبالتالي استخدامها في النفاذ إلى حسابات أخرى. وللسبب ذاته فإن التبديل ما بين كلمتي سر أو ثلاثة وتوزيعها على كل الحسابات غير محبَّذ.
- **أن تتغيّر باستمرار :** من المهم تغيير كلمات السر دوريا، على الأقل مرة كل ثلاثة أشهر. بعد الأشخاص يرتبطون بكلمة السر ولا يغيرونها لسنوات طويلة، هذه عادة سيئة جدا، خصوصا في الحسابات التي تستخدم في العمل، لأنه كلما طال عمر كلمة السر زادت فرصة أن يكون آخرون قد اكتشفوها، ولو أن هذا حدث دون علمك، فإنهم سيظلون قادرين على النفاذ إلى بياناتك دون علمك حتى تغيِّر كلمة السر.

منصور : ماذا إن كنت أثق في شخص ؟ ألا يمكنني أن أخبره بكلمة سرّي ؟

ماجدة : كونك تثق في شخص ما لا يعني أن تثق بالضرورة في قدرته على الحفاظ على كلمة السر، أليس كذلك ؟ ومع أني لن أتعمد أن أسيئ استغلال كلمة سرّك إن أعطيتنيها، إلا أني قد أكتبها في ورقة بهدف مساعدتك على أداء الغرض الذي من أجله أعطيتنيها ! والحقيقة أن هذا قد يكون هو سبب وقوعي في هذه المشكلة في المقام الأول. كما أن الموضوع لا يتعلق بالثقة، فإن كنت أنت الشخص الوحيد الذي يعرف كلمة السر فهذا يقطع سبيل الخلافات وتبادل اللوم إن حدث وانكشفت، وهو ما قد يضر بالثقة في نهاية المطاف. فأنا الآن واثقة أن شخصا ما خمَّن أو كسر كلمة سرّ حسابي البريدي، لأني متيقنة من أني لم أكتبها وأعطها لأحد.

تَذكُّرُ وحفظ كلمات السِّر

بمطالعة قائمة مقومات كلمات السر في القسم السابق قد تتعجب كيف يمكن لشخص ذو ذاكرة عادية، أو اقل من العادية، أن يحفظ في ذاكرته كلمات سرّ عديدة بهذا الطول والتعقيد تتغير باستمرار. النصائح التالية قد تساعد على تأليف كلمات سرٍّ قوية يصعب على الآخرين تخمينها ويتطلب جهدا أكبر لكسرها ببرمجيات القوة الغاشمة.

تذَكُّر كلمات السر القوية

توجد عدة طرق لتنويع الأحرف المدخلة في كلمة السر :

- التنويع في أشكال الأحرف اللاتينية الكبيرة والصغيرة بغير التزام بالقواعد الأصلية :
  "My naME is Not MR. MarSter"
- استبدال أحرف بأرقام : "a11 w()RK 4nD N0 p14y"
- استبدال أحرف برموز : "c@t(heR1nthery3"
- تضمين كلمات من لغات عدة : "Let Them yaklo 1e gateau au ch()colaT"
- كتابة العربية بالأحرف اللاتينية : "al3arabi keda baye5 geddan"
- كتابة كلمات عربية لكن بلوحة المفاتيح مضبوطة على اللاتينية : "Hf, [glf, uhdl ugn kfi]"، لكن لاحظ أن هذه الطريقة قد لا تعمل كما ينبغي عندما يختلف ترتيب لوحة المفاتيح ما بين وقت تأليف كلمة السر والحاجة إلى إدخالها، مثل لوحة المفاتيح الفرنسية أو إن تغيرت ما بين الإنجليزية البريطانية وإنجليزية الولايات المتحدة.

يمكنك طبعا استخدام كل أو بعض تلك الأساليب في الوقت ذاته، وجميعها تساعد على زيادة درجة تعقيد كلمة السر وبالتالي صعوبة كسرها. لكن لاحظ أنه مع أن بعض استبدالات الأحرف الشهيرة، مثل استبدال o و0 أو a و@ قد ضُمنت بالفعل في برمجيات كسر كلمات السر لشيوعها، إلا أنها لا تزال تفيد في زيادة مجال البحث وبالتالي تصعيب الاكتشاف والتخمين.

يمكنك كذلك استخدام أساليب التذكر لتحويل عبارات طويلة سهلة الحفظ إلى كلمات سر معقدة شبه عشوائية، مثلا :

- "To be or not to be? That is the question" يمكن أن تتحوّل إلى "2Bon2BTitQ"
- "We hold these truths to be self-evident: that all men are created equal" يمكن أن تتحول إلى "WhtT2bs-e:taMac="
- "Are you happy today?" يمكن أن تصبح "rU:-)2d@y?"

الأسلوب الناجح هو الذي تستخدم فيه كل ماسبق : أن تبدأ بعبارة أو مجموعة كلمات ذات دلالة خاصة لديك وبالتالي فإنك تحفظها جيدا، ثم أن تجري على أحرفها مجموعة من التحويلات وفق قواعد خاصة تبتكرها بنفسك لنفسك ولا يعلمها سواك. بهذه الطريقة سيكون بوسعك دوما إعادة إجراء العمليات التحويلية الخاصة خطوة خطوة انطلاقا من العبارة الأصلية وصولا إلى عبارة السِّر.

الحفظ الآمن لكلمات السر

مع أن تلك الطرق قد تساعدك على تذكر عدد لا بأس به من كلمات السر، إلا أن التوصية المثالية بتغيير كلمات السر دوريا قد تستنفد حيلتك. لذا فبدلا عن هذا يمكنك استخدام أقوى شكل من

أشكال كلمات السر، وهي الكلمات العشوائية المولدة آليا وبدلا من محاولة تذكرها أن تستعين بأداة تحفظها لك في خزانة خاصة لكلمات السر محمية بالتعمية القوية، مثل كيپاس المشروح استخدامه في دليل الأدوات.

دليل عملي: ابدأ مع دليل كيپاس

إن استخدمت هذه الوسيلة فسيكون عليك أن تؤلف وتتذكر كلمة سرٍّ واحدة قوية لتحمي بها قاعدة البيانات التي تحوي كلمات السر العديدة الأخرى، سواء استخدمت كيپاس (KeePass) أو أداة أخرى مثل Password Safe. وعندها فكلما احتجت لإدخال كلمة سر لحساب ما يمكنك استخراجها سريعا من الخزانة. كيپاس أداة محمولة، أي يمكن نسخها من وإلى شذرة ذاكرة مثل يوإسبي واستخدامها منها مباشرة دون حاجة إلى تنصيب على كل حاسوب، وهو مفيد عند السفر أو عند التنقل ما بين الحواسيب.

هذا الأسلوب مفيد لمن لديه حسابات عديدة، إلا أن المأخذ عليه يتمثل في أنك إن فقدت قاعدة البيانات فقدت كل شيء، وسيكون عليك استرجاع كلمات السر من الخدمات ذاتها واحدة واحدة، إن كانت تتيح إجراء لعمل ذلك. لذا فحفظ نسخة احتياطية من قاعدة بيانات كلمات السر في موضع آمن أمر حيوي. لمزيد من المعلومات عن الحفظ الاحتياطي طالع فصل ٥: "تدارك فقد البيانات"، لكن لحسن الحظ فكون قاعدة بيانات كلمات السر معماة يعني أن سرقة شذرة الذاكرة أو ضياع وسيط يحوي نسخة منها ليس مما يثير الفزع أو يشكل تهديدا بالغا.

المأخذ الثاني، وهو الأهم، أنك إن نسيت كلمة السر التي تحمي خزانة كلمات السر فلا توجد طريقة لاسترجاعها، وإلا ما نصحنا باستخدامها. لذا فاعمل على تأليف كلمة سر قوية يمكنك فعلا تذكرها وقت اللزوم.

منصور : انتظري لحظة ! بما أن كيپاس يستخدم كلمة سرٍّ واحدة لحماية كلمات السر الأخرى العديدة، فكيف يكون هذا آمن من استخدام كلمة سرٍّ واحدة لكل الحسابات وتوفير الجهد ؟

ماجدة : تفكير جيِّد، وهذا يؤكد أهمية حماية كلمة السر الرئيسية، إلا أنه توجد عدة فروقات ؛ فأولا، المهاجم لن يلزمه فقط معرفة كلمة السر، بل كذلك الحصول على ملف قاعدة بيانات كيپاس ذاته، بينما إن كنت تستخدم كلمة سرٍ واحدة لكل حساباتك فعندها يكفيه معرفة كلمة السر. علاوة على أننا نضمن قوة كيپاس في حماية كلمة السر أكثر مما نضمن الخدمات والبرمجيات الأخرى التي تتطلب كلمات سر، فتصميمات بعضها ضعيفة حقا وقد وقعت مسبقا اختراقات موثقة لبعضها، ولا أظنك ترغب في أن يخترق أحدهم موقعا ما ثم يستخدم المعلومات التي حصل عليها منه في اختراق حسابات أخرى. كما أن تغيير كلمة سر كيپاس يسير للغاية.

٤
حفظُ سِرِّية البيانات الحسّاسة

٤. حفظُ سِرِّية البيانات الحسّاسة

النفاذ غير المصرح به إلى البيانات المخزنة على الحاسوب أو وسيط التخزين المحمول يمكن أن يجري عن بعد إن كان المخترق قادرا على التفاعل مع الحاسوب عبر الشبكة، أو ماديا إن كان قادرا على وضع يده على العتاد. تمكن حماية البيانات من الفئة الأولى من التهديدات كما هو مبينٌ في فصل ١: "حماية الحاسوب من البرمجيات الخبيثة ومن المخترقين" ومن الفئة الثانية من التهديدات كما هو مبين في فصل ٢ "الحماية من الأخطار المادية"، إلا أننا يجب أن نعلم أنه لا توجد دفاعات ولا احتياطات لا يمكن اختراقها، لذا فمن الأفضل وضع خطوط دفاع متتالية.

في حال وضع المهاجم يده على العتاد أو وسائط التخزين، بطريق السرقة أو المصادرة أو المغافلة لبرهة، فإن السبيل الوحيد الفَعَّال للدفاع هو إما **التعمية** أو **الإخفاء**، وتوجد أدوات برمجية عِدَّةٌ لتطبيق كلا الأسلوبين، وبعضها **تطبيقات حرة**. البرمجية التي نشرحها في هذا الدليل هي تروكريپت (TrueCrypt) وهي تُستخدم أساسا لتعمية الملفات كما تحوي وظيفة لإخفاء البيانات المعماة.

سيناريو تطبيقي

كلَوديا وپابلو يعملان في منظمة حقوقية في أمريكا الجنوبية، وقد أمضيا أشهرا يجمعان شهادات عيان عن انتهاكات حقوق الإنسان التي ارتكبها الجيش في منطقتهما، وهي شهادات قد يُعرِّض انكشافُها الشهودَ لخطرٍ داهم ومعهم الحقوقيين والناشطين في عدة منظمات تعمل في المنطقة. تلك المعلومات مخزنة في ملفات على حاسوب في المنظمة التي يعملان فيها وهو مُتَّصل بالإنترنت. ولأن كلَوديا حصيفة فيما يتعلق الأمان فقد حفظت نسخة احتياطية من الملفات على قرص مدمج تحتفظ به في مكان آمن بعيدا عن المكتب.

ما يتناوله هذا الفصل

- تعمية البيانات المخزنة في الحاسوب
- المخاطر التي قد تتعرض لها جرّاء استخدام التعمية
- حماية البيانات على وسائط التخزين المحمولة تحسبًا لسرقتها أو فقدها
- الخطوات الممكن اتِّباعها لإخفاء البيانات عن المخترقين الماديين أو عن بعد

تعمية البيانات

پابلو : لكن حاسوبي تحميه بالفعل كلمة سِر الولوج إلى وِندوز، ألا يكفي هذا ؟

كلَوديا : الحقيقة أن كلمة سر الولوج إلى وندوز سهلة الكسر، علاوة على أن من يضع يده على الحاسوب لمدة تكفي لأن يقلعه باستخدام قرص حي يمكنه نسخ البيانات التي يريد دونما حاجة إلى التعامل مع ويندوز بتاتا ؛ وإن كان بوسع المهاجم أخذ الحاسوب لمدة أطول فالأمر أسهل عليه. ليست كلمات سر وندوز وحدها هي ما لا يعتمد عليها، بل كذلك كلمات سر تطبيقات مثل ميكروسوفت ورد أو أدوبي أكروبات.

تعمية البيانات يشبه وضعها في خزانة قوية لها مفتاح، وحدهم من لديهم المفتاح أو يعرفون توليفة القفل يمكنهم النفاذ إلى محتوياتها. هذا المثال ينطبق بالذات على تروكريت (TrueCrypt) والأدوات المشابهة التي تعين على إنشاء حاويات آمنة تسمى "مجلّدات مُعماة" عوضا عن تعمية كل ملف على حدى. تلك المجلدات المعماة يمكنها استيعاب عدد كبير من الملفات والأدلة، إلا أنها لا تحمي أي ملف محفوظ في أي موضع خارجها على الحاسوب أو في أي وسيط تخزين محمول.

دليل عملي: ابدأ مع دليل تروكريت

توجد أدوات ومنظومات أخرى يمكنها توفير التعمية القوية ذاتها التي يوفرها تروكريت، وبعضها برمجيات حرة كذلك، مثل FreeOTFE إلا أن تروكريت يتميز بكونه يَسِر الاستخدام وبتعدد الوظائف المفيدة، إلى جانب الميزة الأهم وهي وظيفة إخفاء البيانات المعماة المشروحة في قسم إخفاء البيانات الحساسة. وفي كل الأحوال فإن جميع تلك البدائل تتفوق على وظيفة التعمية المُتَضَمَّنة في ويندوز.

بابلو : حسن، لقد أقلقتني. ماذا عن المستخدمين الآخرين للحاسوب ذاته ؟ هل يعني هذا أنهم قادرون على الاطلاع على ملفاتي التي أحفظها في دليل "مستنداتي"

كلَوديا : تعجبني طريقة تفكيرك. فإن كانت كلمة سر الولوج إلى وندوز لا تحميك من المخترقين فكيف لها أن تحميك ممن لديهم حسابات على الحاسوب ! الحقيقة أن المستخدمين الذين ليست لديهم صلاحيات إدارية في النظام لا يمكنهم الاطلاع على ملفات المستخدمين الآخرين ماداموا يستخدمون النظام، وذلك لأن نظام التشغيل يفرض تطبيق صلاحيات النفاذ على الجميع مادام هو المسيطر على الحاسوب وما يتصل به من وسائط تخزين، لذا يلجأ المخترقون الذين يمكنهم وضع يدهم على العتاد إلى إقلاع نظام تشغيل مختلف أو وصل وسيط التخزين بحاسوب آخر لتجاوز هذه الطبقة من الحماية. وهذا ينطبق على جميع نظم التشغيل. لكن تذكر أنه في بعض إصدارات وندوز يكون الوضع المبدئي لدليل "مستنداتي" أنه مشترك، كما أن بعض نظم الملفات لا تدعم تحديد صلاحيات النفاذ ؛ وتذكر كذلك أن من لديهم صلاحية المدير في النظام يمكنه دوما فعل أي شيء. وفي هذه الحالات فإن التعمية هي السبيل الوحيد.

نصائح لاستخدام تعمية الملفات بأمان

تخزين البيانات السرية أو الخاصة أمر محفوف بالمخاطر لك ولمن يعملون معك. تساعد التعمية على التقليل من تلك المخاطر إلا أنها لا تلغيها. الخطوة الأولى لحماية البيانات الحسّاسة هي تقليل الكم المحفوظ منها. فما لم يكن لديك سبب وجيه لتخزين ملف أو فئة معينة من البيانات فلا

تحفظها. (طالع فصل ٦ "تدمير البيانات الحسّاسة" للمزيد عن هذا) الخطوة التالية هي تعمية ما يجب الاحتفاظ به من ملفات باستخدام أداة مثل تروكريت.

كلَوديا : حسن، ربما كنا لا نحتاج إلى حفظ البيانات التي تكشف عن هويات الشهود، ما رأيك ؟

بابلو : أوافقك، ربما كان علينا بالقدر النزير اللازم، مثلا إن كان اتخاذ إجراءات قانونية مطلبا في المستقبل أو لتوثيق تاريخي أكثر مصداقية.

إخفاء البيانات

إحدى مساوئ وجود خِزانة في المكتب أو البيت هو أنها تكون بادية وقد تلفت انتباها غير مرغوب فيه. وبالمثل تكون لدى بعض الناس مخاوف معقولة من أن يدينوا أنفسهم قانونيا باستخدام التعمية، ومع أن المبررات المشروعة لاستخدام **التعمية** أكثر من الدوافع الإجرامية فإن هذا لا يقلل من خطر التجريم القانوني. يوجد سببان رئيسيان قد يدفعانك لإعادة التفكير في استخدام التعمية، وأدوات مثل تروكريت ؛ أولهما خطر الإدانة القانونية، وثانيهما لفت الانتباه إلى موضع حفظ أكثر بياناتك حساسية.

خطر الإدانة القانونية

استخدام التعمية مُجَرَّمٌ في بعض القضاءات، وهذا قد يعني أن مجرد تنزيل أو تنصيب أو استخدام برمجيات التعمية قد يكون جريمة في حد ذاته ؛ وفي حال كون الشرطة أو الجيش أو المخابرات أو الأجهزة الأمنية الأخرى من ضمن أولئك الذين تسعى لحماية البيانات عنهم فإن مخالفة تلك القوانين قد يهيئ ذريعة للتحقيق في نشاط منظمتك أو مساءلتك قانونيا ؛ والواقع أن التهديدات من هذا النوع قد لا تكون لها علاقة بمدى قانونية استخدام التعمية على الإطلاق، إذ قد يكون مجرد ربط شخصك أو منظمتك باستخدام التعمية كافيا لتعريضك لاتهامات إجرامية، بغض النظر عن طبيعة البيانات المُعمَّاة ؛ وفي هذه الحالة عليك التَّمَعُّن في مسألة استخدام مثل هذه الأدوات وما إذا كانت مناسبة لحالتك. إن كان هذا هو الحال فقد تكون لديك بعض الخيارات البديلة التالية :

- تفادي استخدام برمجيات تأمين البيانات تماما، وهو ما يعني أن تحفظ وحَسْبُ البيانات غير السِّرية أو أن تبتكر نظاما من الشفرات لتمويه البيانات السرية.
- استخدام تقنية **الاستگانوگرافيا** لإخفاء البيانات السرية عوضا عن تعميتها. توجد أدوات تطبق تقنيات عديدة لتحقيق هذا، ويتطلب استخدامها بعض الدراسة والإعداد، كما يجب التكتم بقدر الإمكان على الأدوات والتقنيات التي تستخدمها، لأنه على غير التعمية التي يكون السر الوحيد فيها هو المفتاح أو كلمة السر ؛ ومع هذا يبقى احتمال الإدانة من قِبَل كل من يكتشف وسيلة لاستخراج البيانات المخفاة.

- حفظ البيانات الحساسة كمرفقات في حساب بريد إلكتروني على الوب مؤَمَّن، إلا أن هذا يتطلب اتصالا جيدا بالإنترنت وخبرة معقولة لإيجاد الخدمة والأدوات المناسبة، كما يتطلب حرصا لعدم حفظ البيانات السرية على وسائط غير مؤمنة وتركها عليها.
- حفظ البيانات الحساسة بعيدا عن الحاسوب، مثلا على شذرات ذاكرة يواِسبي أو وسيط محمول آخر ؛ إلا أن هذه الوسائط أكثر عرضة من الحواسيب للضياع والمصادرة، كما أن حمل بيانات حسّاسة والتجول بها قد يُشكِّل خطرا على حاملها، وهو ليس محبذا.

عند اللزوم يمكن اتّباع عدد من هذه الأساليب مع بعضها ؛ ومع هذا ففي حالات خشية التجريم القانوني فقد يكون من الأنسب استخدام التعمية على أي حال مع السعي إلى تمويه وجود البيانات المُعمّاة بقدر المستطاع.

مثلا يمكن إخفاء وجود **مجلدات** تروكريبت المعماة بتسميتها بحيث تبدو كملفات من نوع آخر، فمثلا استخدام امتداد الاسم iso. لتنكيرها في هيئة ملف صورة قرص مدمج يناسب ملفات المجلدات التي يتراوح حجمها حول ٧٠٠ ميجابايت، يمكن كذلك استخدام امتدادات ملفات صيغ الفيديو والأوديو، مع ملاحظة أن هذه الملفات لن تعمل مع المشغلات أو التطبيقات المستخدمة أصلا لأي من الأنواع المذكورة. هذا يشبه إلى حد ما إخفاء الخِزانة خلف لوحة على الجدار، فهو لن يصمد في وجه الباحث المتمعن إلا أنه على الأقل لن يجلب انتباها زائدا.

يمكن كذلك تغيير اسم ملف برمجية تروكريبت ذاته والمجلد الحاوي ملفاته وحفظها في غير الموضع الذي تنصب فيه عادة البرمجيات، وحفظها عوضا عن ذلك كملف عادي على شذرة ذاكرة واستخدامها منها بلا تنصيب. فصل تروكريبت يشرح كيفية عمل ذلك.

خطر كشف وجود البيانات الحسّاسة

عادة ما يكون قلقنا من احتمال أن نضبط متلبسين باستخدام برمجيات التعمية أقل من قلقنا من أن وجود حاوية بيانات معماة يشير بجلاء إلى وجود البيانات الأكثر حساسية والتي نرغب في حمايتها بأكثر ما يمكن. ومع أنه لا يمكن لغير من يحوز المفتاح الاطلاع عليها إلا أن المهاجم وقد صار يعرف بوجودها وأنك اتخذت إجراءات لحمايتها قد يصبح أكثر إصرارا على استخراجها، مما قد يعرضك لتهديدات غير تقنية، مثل التهديد أو الابتزاز أو الاستجواب مع التعذيب، وهو احتمال وارد في البلاد التي يمكن أن تعمل فيها الجهات الأمنية خارج حدود القانون ويمخفى عن الرقابة، كما أنه أسهل وقد يكون أكثر جدوى من محاولة استخدام الأساليب التقنية لاكتشاف كلمات السر وكسر التعمية. هذا هو السياق الذي قد تفيد فيه وظيفة دعم **حُجَّة الإنكار** في تروكريبت.

وظيفة حجية الإنكار إحدى مميزات تروكريبت، وهي توظف نوعا خاصا من **الاستگانوگرافيا** لتمويه وجود البيانات الحساسة المعماة خاف بيانات أخرى معماة أقل حساسية ؛ وهو مماثل لوجود جيب سري في خزانة مقفولة بمفتاح، بحث إذا تمكن المهاجم من الحصول على المفتاح أو إجبارك على فتحها تحت التهديد فسيجد ما يمكن أن يظنه المواد المطلوبة وقد يدفعه هذا إلى الاكتفاء بما حصل عليه دون أن ينتبه إلى وجود ما يهمك إخفاؤه حقا في الجيب السري. ولأنك وحدك تعرف بوجود الجيب السري يمكنك أن تنكر وجود أي شيء آخر، لو سُئلت، وقد يقنع هذا المهاجم. قد يفيد هذا في الحالات التي تُجبر فيها على الإفصاح عن كلمة السر لسبب ما، خشية تهديد مادي أو قانوني، وحجية الإنكار تمنحك خيار مواصلة حماية البيانات شديدة الحساسية مع

حماية نفسك أو غيرك من الخطر. لكن كما هو موضح في قسم خطر الإدانة القانونية فإن هذا الأسلوب قد يكون غير مجدٍ إذا ما كان لمجرد استخدام التعمية عواقب وخيمة.

تعمل وظيفة دعم حجية الإنكار بطريق إنشاء مجلد مُعَمَّى مخفي داخل مجلد مُعمّى آخر، ويلزم لفتح المجلد المخفي والنفاذ إلى محتوياته معرفة كلمة سر تختلف عن المستخدمة لفتح المجلد الخارجي، لذا فإن تمَكَّن مهاجم من فتح المجلد الخارجي – بتعاونك، لأن كسر التعمية غير مجدٍ – فإنه حتى وإن كان ذا خبرة تقنية فلن يمكنه التيقن من وجود أو عدم وجود مجلد مخفي داخله، ولا إثبات ذلك ما دُمتَ تنكره، حتى مع أنه قد يعرف أن مثل هذه الوظيفة توجد في تروكريبت، مما قد يدفعه إلى تركك لحالك، إلا أن هذا كما هو جليٌّ غير مؤكد وراجع إلى سلطة المهاجم الذي يملك إكراهك.

يستخدم عديدون تروكريبت للتعمية دون استخدام وظيفة دعم حجية الإنكار، والمُجمَع عليه إلى الآن أنه لا يمكن حتى بطرق التحليل التقني تحديد وجود مجلد مخفي داخل أي مجلد تروكريبت مُعمّى من عدمه ؛ هذا إن اتبعت الطريقة السليمة والتوصيات لاستخدامه لتلافي ترك مؤشرات ثانوية قد تشير إلى وجوده أو استخدامه، مثل مدخلات في سجلات التطبيقات أو اختصارات على سطح المكتب أو قوائم آخر المستندات.

كلَوديا : حسن، لنضع بعض الملفات غير الهامة في المجلد الخارجي وبعدها ننقل ملفات شهاداتنا الحسّاسة إلى المجلد المخفي في داخله. أليديك بعض الملفات القديمة أو ما شابه ؟

بابلو : كنت أفكر في هذا أيضا..أقصد..أن الفكرة هي أن نفصح عن كلمة السِّر التموهية إن لم يكن أمامنا خيار سوى ذلك، صحيح ؟ لكن لكي تكون هذه الحيلة مقنعة ينبغي أن تبدو تلك الملفات هامة، أليس كذلك ؟ وإلا فلم تجشمنا عناء تعميتها ! ربما وجب علينا أن نضع فيها مستندات مالية غير ذات علاقة بالموضوع، أو كلمات سر حسابات على مواقع حقيقة لكن غير هامة، أو تقارير عن العمل لا يحوي بيانات سرية يمكن أن تهدد أحدًا.

٥
تَدارُكُ فَقْدِ البيانات

٥. تَدارُكُ فَقْدِ البيانات

كل طريقة جديدة في تخزين البيانات الرقمية أو نقلها تنجم عنها مخاطر جديدة بتلفها أو ضياعها أو سرقتها والتنصت عليها، ويمكن لحصيلة سنوات من العمل أن تُفقد في لحظة، نتيجة سرقة، أو إهمال لحظي، أو المصادرة، أو بسبب قصور في تقنية تخزين البيانات. تذكّر أن التقنيات البدائية بالنقش على الحجر والكتابة على البردي لا تزال آثارها باقية اليوم بعد آلاف السنوات بينما تتلف كل يوم مشغلات الأقراص الصلبة وتخدش الأقراص المدمجة مضيعة ملايين الصفحات، ليس كلها هاما أو لا يمكن تداركه، لحسن الحظ. يشيع بين التقنيين أن المسألة ليست "ما إن كنت ستفقد بياناتك" بل هي بالأحرى مسألة "متى ستفقد بياناتك"، لذا فمن الأفضل أن تكون محتاطا لهذه اللحظة، فربما كانت في عنوان الفصل مغالطة، إذ أن **تدارك** فقد البيانات غير مضمون ما لم نكن قد احتطنا قبل وقوعه بحفظ نسخة احتياطية منها ودرسنا كيفية استرجاعها وقت الحاجة. عادة ما يكون اليوم الذي تتأكد فيه من أهمية الحفظ الاحتياطي هو اليوم الذي تحتاج فيه إلى استرجاع بيانات.

و بالرغم من كونه واحدا من أساسيات تشغيل نظام معلومات سليم فإن تأليف سياسة للحفظ الاحتياطي ليست سهلة كما تبدو، وقد تتطلب جهدا بالغا تخطيطا لأسباب عِدَّة، منها : الحاجة إلى حفظ الوسائط التي تحوي المحفوظات في مواضع مادية مختلفة ؛ وأهمية الحفاظ على سرية المحفوظات ؛ وصعوبة التنسيق بين الأشخاص الذين يتشاركون في المعلومات مستخدمين حواسيب ووسائط تخزين مختلفة. إلى جانب أساليب الحفظ واسترجاع المحفوظات يتناول هذا الفصل أداتين هما كوبيان باكأب (Cobian Backup) وأنديليت پلس (Undelete Plus).

سيناريو تطبيقي

إلينا ناشطة بيئية في دولة ناطقة بالروسية، وقد بدأت بإنشاء موقع على الوب سيوظف الصور والفيديو والخرائط والنصوص لتسليط الضوء على الأنشطة غير المشروعة التي تدمر الغابات في المنطقة، وهي تجمع منذ سنوات وثائق ومحتوى وبيانات جغرافية عن قطع الأشجار، ومعظم تلك البيانات محفوظ في حاسوب عتيق يشتغل بوندوز في مكتب المنظمة الأهلية التي تعمل بها. وبينما تعمل على تصميم الموقع اكتشفت أهمية حفظها تحسبا لعطل حاسوبها، خاصة إذا حدث هذا قبل أن تنشر كل شيء على الموقع، وكذلك للحفاظ على أصول الملفات. وبما أن أفرادا غيرها في المنظمة يستخدمون الحاسوب أحيانا فهي كذلك ترغب في معرفة كيفية استرجاع الملفات إذا ما حذفها أحد أو بعضها بطريق الخطأ. وهي لهذا تستعين بابن أختها نيكولاي ليعينها على تطوير سياسة للحفظ الاحتياطي.

ما يتناوله هذا الفصل

- تنظيم وحفظ البيانات احتياطيا
- موضع استرجاع المحفوظات

- تأمين المحفوظات
- استرجاع الملفات المحذوفة بطريق الخطأ

حصر وتنظيم البيانات

يمكن لكثير من المخاطر أن تؤدي إلى ضياع كل بياناتك أو بعضها، من عدوى **البرمجيات الخبيثة** وهجمات **المخترقين** إلى تذبذبات التيار الكهربي، مرورا بالسرقة والمصادرة، وصولا إلى تلف العتاد، وانهيار نظام التشغيل، وغيرها. الاستعداد لمواجهة الكارثة لا يقل أهمية عن العمل لتلافيها.

إلينا : أدرك أهمية الحفظ الاحتياطي يا نيكولاي، لكن ألا يعني هذا أنني يجب أن أوكل مهمة إعداده إلى غيري ؟ ما أقصده هو..هل سيكون لديَّ الوقت والموارد والخبرة الكافية لإجراءه بنفسي ؟

نيكولاي : أعرف أنك ستبلين بلاء حسنا. وضع خطة للحفظ الاحتياطي قد تتطلب بعض التفكير إلا أنها لا تستغرق الكثير من الوقت أو المال، ومقابل احتمال فقد كل البيانات فإن هذا يُعدُّ مجديا، أليس كذلك ؟ إضافة إلى أن الحفظ الاحتياطي هو حتما إحدى المهام التي ترغبين في أداءها بنفسك ؛ فما لم يكن من تعتمدين عليه في ذلك شديد الحرص والدقة وعارفا بالمواضع التي تحفظين فيها بياناتك، كان من الأفضل أن تؤديها بنفسك.

الخطوة الأولى في وضع **سياسة للحفظ الاحتياطي** هي حصر مواضع وجود بيانات العمل والبيانات الشخصية. فعلى سبيل المثال، قد يكون البريد الإلكتروني محفوظا على **خادوم** مقدم الخدمة، أو على حاسوبك، أو كليهما، كما قد يكون لديك أكثر من حساب بريدي. وهناك كذلك الوثائق المهمة في الحواسيب التي تستخدمينها، في المكتب والمنزل، أو التي أنشأتها باستخدام خدمات على الإنترنت وحفظتها عليها. توجد أيضا أدلة العناوين، وسِجلات المحادثات، وإعدادات البرمجيات. كما يمكن أن توجد معلومات محفوظة في وسائط محمولة مثل ذواكر يوإسبي وسوّاقات الأقراص المحمولة وأقراص الليزر المُدْمَجَة، وحتى الأقراص المرنة القديمة. تحوي الهواتف المحمولة قوائم معارف وسبل الاتصال بهم، وقد تكون فيها رسائل نصّية هامة. إن كان لديك موقع على الوب فقد يحوي كثيرا من المقالات المتجمعة عبر السنوات. ولا تنسي المعلومات غير الرقمية مثل الدفاتر والخطابات.

بعدها، عليك تحديد أي تلك الملفات هو الأصل وأيها النسخة. الأصل هو الإصدارة الأحدث من ملف أو مجموعة ملفات والتي ستحررينها لتحديثها عندما يتغير محتواها من المعلومات. هذا لا ينطبق على الملفات والوثائق التي لا توجد منها سوى نسخة واحدة، إلا أنه هام في الحالات الأخرى. أحد أكثر سيناريوات فقد البيانات شيوعا هو الذي تُحدَّث فيه إحدى نسخ وثيقة ما ثم تتلف أو تحذف في حين تُستبقى نسخ منها لم تكن قد حُدِّثت. فلو تصورنا أنك سافرت في رحلة عمل وأخذت على ذاكرة يوإسبي نسخة من ملف جدول تكاليف رحلاتك، في هذه اللحظة تكون هذه النسخة هي الأصلية لأن الحفظ الاحتياطي للنسخ الأخرى الباقية في حاسوب المكتب لن يكون

مفيدا، ويجب فور عودتك أن تنسخ هذه الوثيقة التي كانت معك فوق الأخرى التي بقيت في المكتب لتأخذ طريقها المعتاد في دورة الحفظ. وعموما حاول أن لا توجد من الوثيقة الواحدة أكثر من نسخة **غير نسخة المحفوظة الاحتياطية** التي لا تعمل عليها مباشرة.

توجد كذلك اعتبارات وجود عدة وثائق متشابهة من ذات المحتوى، كالنسخ المختصرة أو المخففة التي ننتجها لاستعمالات خاصة. فمثلا، قد نقتطف أجزاء من تقارير أو مشاريع لاستعمالها في غرض معين، أو قد تولِّد صورا قليلة **الميز** أو مُصغَّرات من صور فوتوغرافية رقمية لنشرها على الوب. مسألة اعتبار هذه الملفات وثائق مستقلة يعتمد على مقدار الجهد المطلوب لعملها ومدى تكرار الحاجة إليها.

حاولي كتابة قائمة بمواضع وجود كل الأصول والنسخ من بياناتك. سيساعدك هذا على استبيان احتياجاتك والبدء في وضع سياسة الحفظ الاحتياطي. الجدول التالي مثال مبسط على هذا، والأغلب أن قائمتك ستكون أطول وستحوي وسائط تخزين متنوعة وأنواع بيانات متنوعة.

نوع البيانات	أصل/نسخة	وسيط التخزين	الموضع
وثائق رقمية	أصل	السواقة الصلبة للحاسوب	المكتب
بضع وثائق رقمية هامة	نسخة	ذاكرة يوإسبي	معي
قواعد بيانات التطبيقات (دليل عناوين، رُزنامة) وغيرها	أصل	السواقة الصلبة للحاسوب	المكتب
بعض وثائق رقمية	نسخة	أقراص مدمجة	المنزل
البريد والعناوين	أصل	حسابي عند مقدم الخدمة	الإنترنت
رسائل نصيّة وأرقام هواتف	أصل	الهاتف المحمول	معي
وثائق مطبوعة (عقود، فواتير)	أصل	دُرج المكتب	المكتب

قواعد بيانات التطبيقات هي الملفات التي تنتجها وتحفظ فيها البرمجيات المختلفة بياناتها أثناء استخدامها، أحيانا دون تدخل واضح من المستخدم بتحديد اسمها وموضع حفظها ؛ وهي تضم إضافة إلى الأمثلة السابقة ملفات برمجيات الحسابات ومُدراء المعلومات الشخصية.

يظهر من الجدول أن :

- الوثائق التي ستنجو إذا انهار القرص الصلب في حاسوب المكتب هي النسخ التي في ذاكرة يوإسبي والتي على الأقراص المدمجة في المنزل.
- ليست لديك نسخة خارج الإنترنت من رسائلك البريدية أو دليل عناوين معارفك، لذا فإن نسيت كلمة السر أو غيَّرها غيرك بقصد الإضرار بك فستفقدها.
- ليست لديك أي نسخ من البيانات التي في الهاتف المحمول.
- ليست لديك نسخ، سواء رقمية أو مستنسخات، من الوثائق الورقية.

وضع استراتيجية الحفظ الاحتياطي

إجراء حفظ احتياطي يحمي كل أنواع البيانات التي في الجدول السابق يتطلب برمجيات وإجراءات. الغرض هو التيقُّن من أن كل بيان محفوظ في موضعين مختلفين على الأقل.

الوثائق الرقمية

احفظ نسخة كاملة من كل الوثائق المخزنة في الحاسوب باستخدام أداة مثل كوبيان باكَب (Cobian Backup) المشروح في فصل من "دليل الأدوات". خزِّن المحفوظة في وسيط تخزين محمول ليمكن نقله إلى موضع آمن غير الموضع الأصلي للبيانات. قد يكون من اليسير استخدام أقراص الليزر المدمجة سي‌دي أو دي‌في‌دي لهذا الغرض عوضا عن سواقة أقراص صلبة محمولة أو ذاكرة يو‌إس‌بي لئلا تتعرض لاحتمال فقد المحفوظة القديمة قبل تمام إنجاز الأحدث، إلا إن كان لديك عدد من الأقراص بحيث توجد محفوظة واحدة على الأقل في موضع آمن في أي لحظة. ولأن هذا النوع من الوثائق عادة ما يحوي بيانات حسّاسة فمن الأفضل حمايةُ المحفوظةِ بالتعمية كما هو مشروح في "فصل حفظ سرية البيانات الحسّاسة" وفي "دليل استخدام تروكريت".

قواعد بيانات البرمجيات

بعد تحديد مواضع قواعد برمجيات التطبيقات يمكن معاملتها مثل الوثائق الرقمية.

البريد الإلكتروني

بدلا من النفاذ إلى البريد بطريق الوب حصرا يمكن استخدام عميل بريد مثل ثَندَربِرد وضبطه ليجلب البريد من الخادوم. توفر معظم خدمات البريد هذه الوظيفة مجانا، وتنشر إرشادات لكيفية استخدام عملاء البريد الشهيرة معها. كيفية أداء هذا مشروحة في "دليل استخدام ثندربرد (*Thunderbird*)". لكن راع أن جلب وحفظ البريد محليا يستقدم مخاطر إضافية، ومن الأفضل حمايته باستخدام التعمية كما هو مشروح في فصل ٤: "فصل حفظ سريِّة البيانات الحسّاسة".

محتويات الهاتف المحمول

لحفظ أرقام الهواتف والرسائل النصية التي في الهاتف المحمول يمكن وصله بالحاسوب باستخدام البرمجيات الملائمة، وهذه عادة ما يوفرها الصانع في موقعه. هذه الوظيفة موجودة في أغلب الهواتف الحديثة، إلا أنها قد تتطلب شراء كابل خاص. تتيح بعض الهواتف – خصوصا الحديثة – وظيفة الاتصال بطريق بلوتوث (BlueTooth). وكبديل يمكن باستخدام الهاتف نسخ البيانات من ذاكرة شريحة SIM العادية إلى ذاكرة الهاتف الداخلية ثم مرة أخرى إلى ذاكرة شريحة SIM احتياطية، وهو حل جيد للطوارئ ؛ لكن احرص على تأمين شريحة SIM الاحتياطية. كما تتيح بعض طرز الهواتف استخدام شريحة ذاكرة فلاش، وهذه تسهل الحفظ الاحتياطي كثيرا.

الوثائق المطبوعة

حاول بقدر الإمكان مسح الوثائق الورقية وحفظ الوثائق الإلكترونية الناتجة مع باقي الوثائق الإلكترونية كما هو موضّح أعلاه.

في النهاية ستكون قد أعدت توزيع استخدامات وسائط التخزين بما يزيد من حصانة بياناتك على الكوارث.

نوع البيانات	أصل/نسخة	وسيط التخزين	الموضع
الوثائق الإلكترونية	أصل	السواقة الصلبة في الحاسوب	المكتب
الوثائق الإلكترونية	نسخة	أقراص مدمجة	المنزل
بعض الوثائق الإلكترونية الهامة	نسخة	ذاكرة يو‌إس‌بي	معي

نوع البيانات	أصل/نسخة	وسيط التخزين	الموضع
قواعد بيانات التطبيقات	أصل	السواقة الصلبة في الحاسوب	المكتب
قواعد بيانات التطبيقات	نسخة	أقراص مدمجة	المنزل

نوع البيانات	أصل/نسخة	وسيط التخزين	الموضع
رسائل البريد والعناوين	نسخة	حساب البريد	الإنترنت
رسائل البريد والعناوين	أصل	ثندربرد على حاسوب العمل	المكتب

نوع البيانات	أصل/نسخة	وسيط التخزين	الموضع
رسائل نصية وبيانات اتصال	أصل	الهاتف المحمول	معي
رسائل نصية وبيانات اتصال	نسخة	السواقة الصلبة في الحاسوب	المكتب
رسائل نصية وبيانات اتصال	نسخة	SIM احتياطية	المنزل

نوع البيانات	أصل/نسخة	وسيط التخزين	الموضع
وثائق مطبوعة	أصل	دُرج المكتب	المكتب
وثائق ممسوحة	نسخة	أقراص مدمجة	المنزل

إلينا : أعرف أشخاصا يحفظون كل وثائقهم الهامة في حساب البريد الإلكتروني، مثل جيميل بطريق إرفاقها برسائل يرسلونها إلى أنفسهم، فهل يصلح هذا كموضع مختلف لحفظ المحفوظات ؟

نِيكولاي : قد يعين هذا في عملية استرجاع وثيقة أو اثنتين، لكنه نظام متعب إذا ما اعتمدت عليه لكل شيء. كم وثيقة يمكنك حفظها أسبوعيا إن فعلت هذا ؟ وكيف ستديرين النسخ المتقادمة ؟ كما ينبغي عليك أن تأخذي في الحسبان كون البريد مراقبا، وسيكون عليك استخدام اتصال آمن بمقدم الخدمة. استخدام هذا الأسلوب باتصال *HTTPS* المؤمن لحفظ ملفات قليلة العدد والتغير، مثل ملف حاوية تروكريبت ذي حجم معقول، أو لحفظ ملف خزانة كلمات سر كِيپاس قد يكون معقولا، لكني لا أتصور أن يكون هذا حلا شاملا للحفظ الاحتياطي.

إجراء الحفظ الاحتياطي

من بين الأنواع المختلفة للبيانات التي تناولناها فإن الوثائق الرقمية هي عادة أكثر ما يشغل بال من يعملون على وضع سياسة للحفظ الاحتياطي. المقصود بالوثائق الإلكترونية هو تلك التي يعمل عليها مستخدم الحاسوب بأن يفتحها بنفسه لتحريرها بتطبيق ما، إما بأن ينقر على أيقونتها أو من أمر افتح من قائمة أوامر التطبيق. وهي تشمل وثائق معالجات الكلمات — بما فيها الوثائق النصية الصرفة بلا تنسيق، والعروض التقديمية، وجداول الحسابات، وملفات PDF، وغيرها.

إضافة إلى حفظ الوثائق الإلكترونية ينبغي حفظ قواعد بيانات التطبيقات، ومع أنها أيضا ملفات رقمية، إلا أنها على غير الوثائق الإلكترونية لا يتعامل معها المستخدم مباشرة، فلا يفتحها ولا يحفظها عند انتهاء تحريرها، بل تستخدمها التطبيقات تلقائيا لحفظ بيانات المستخدم التي يعالجها التطبيق، كلٌ حسب وظيفته. بعض التطبيقات تحفظ مبدئيا قواعد بياناتها في ذات الموضع الذي يحفظ فيه المستخدم وثائقه، أو يمكن ضبطها لتفعل ذلك ؛ فإن لم يكن ذلك متاحا فقد تجد أن معظم التطبيقات الحديثة العاملة في وندوز تحفظ قواعد بياناتها في أدلة فرعية تحت دليل حساب المستخدم، وعندها ينبغي أن تُضَمِّنَ تلك الملفات والأدلة في المحفوظات الاحتياطية دوريا.

مخزن البريد الذي يحفظه تطبيق عميل البريد الإلكتروني مثل ثندربرد هو أحد أمثلة قواعد بيانات التطبيقات. في بعض الحالات فإن برمجيات تشغيل الوسائط واستعراض الصور تدير ملفات الوسائط وتحفظها باعتبارها مدخلات في قاعدة بيانات خاصة، ويكون عليك اكتشاف موضعها على القرص الصلب وإضافته إلى المحفوظة.

وسائط التخزين

للتخطيط الجيد للحفظ الاحتياطي ينبغي معرفة نوعية وسعات الوسائط المستخدمة في الحفظ وأخذ ذلك في الحسبان.

الأقراص المدمجة - سي‌دي (CD)

الأقراص القياسية تخزن ٦٥٠ ميجابايت، إلا أن معظم الأقراص الموجودة في الأسواق حاليا يمكنها أن تخزن ٧٠٠ ميجابايت وهي متوافقة مع القياسية. يتطلب التسجيل مسجلة أقراص ليزرية وأقراصا شاغرة. إضافة إلى أقراص التسجيل مرة واحدة (CD-R) توجد أقراص قابلة لإعادة الكتابة (CD-RW) يمكن محوها وإعادة استخدامها لعدد من الدورات. لاحظ أن عمر الأقراص المدمجة الجيدة يتراوح ما بين خمس إلى عشر سنوات، وأقل من ذلك للأقراص التي يمكن إعادة التسجيل عليها. فإن نويت الاحتفاظ ببيانات على أقراص لمدد أطول من ذلك سيكون عليك نقلها من الأقراص القديمة إلى أحدث منها كل بضع سنوات، أو شراء أقراص خاصة ذات عمر طويل، وهي أغلى ثمنا. لاحظ كذلك أن الأقراص المدمجة بالغة الرخص قد يكون كثير منها تالفا من البداية، لذا يفضل اختبارها بعد نسخ البيانات إليها.

أقراص الفيديو الرقمي - دي‌في‌دي (DVD)

هي نوع أحدث من أقراص الليزر المدمجة يستوعب النوع الأقل في السعة منها ٤,٧ جيجابايتا من البيانات، وصفاتها مشابهة للأقراص المدمجة التي حلّت محلها لدى كثير من المستخدمين، إلا أنها تتطلب قارئات ومسجّلات خاصة بها، ومعظمها متوافقة رجوعا مع الأنواع الأقدم.

شذرات ذاكرة يوإسبي (USB)

وسائط تخزين من نوع فلاش تتصل بالحواسيب بطريق منافذ يوإسبي التي أصبحت قياسية في الحواسيب الحديثة. توجد شرائح الذاكرة هذه في أشكال عديدة من صانعين عديدين، وسِعة المنتجات الموجودة منها في الأسواق تتزايد باضطراد ويتناقص سعرها كذلك باضطراد، وستماثل قريبا سعاتها سعات سوّاقات الأقراص الصلبة الموجودة حاليا، وقد تحل محلها في بعض الاستخدامات. توجد كذلك طرز منها ذات وظائف إضافية مثل دعم التعمية لحماية المحتويات من الفضوليين، لكن ما لم تكن متيقنا من كفاءة النظام المستخدم في مثل هذه الحالات فمن الأفضل الاعتماد على منظومات تعمية خارجية موثوق بها. مثل كل وسائط التخزين لشرائح الذاكرة عمر تشغيلي تفقد بعده قدرتها على حفظ واسترجاع البيانات وتتزايد احتمالات تلف البيانات، ويحدد عمرها عدد دورات القراءة/الكتابة التي تتحملها مكوناتها ؛ ومتوسط عمر الأنواع الجيدة مع الاستخدام النمطي يقدّر بعشر سنوات.

خادوم بعيد

يمكن **لخادوم** ملفات على الشبكة أن يكون ذا سعة كبيرة جدا، إلا أن توفر الاتصال الشبكي عند الحاجة وسرعة الاتصال واعتماديته عوامل ينبغي أخذها في الحسبان عند التفكير في استخدام هذا الأسلوب. راعِ أن وجود خادوم ملفات على الشبكة المحلية في المكتب قد يكون أسرع عند الاستخدام من خادوم تتصل به عبر الإنترنت، إلا أنه لا يستوفي وجوب وجود النسخة الاحتياطية في موضع بعيد عن البيانات الأصلية. توجد خدمات تخزين ملفات مجانية على الإنترنت بسعات وشروط مختلفة، كما توجد خدمات مدفوعة عديدة بجودة ومميزات مختلفة تتغير باستمرار، لكن ينبغي تعمية المحفوظات قبل رفعها إلى خواديم على الإنترنت، وذلك لئلا تخضع لسلطة مقدم الخدمة أيًا كان.

برمجيات الحفظ الاحتياطي

كوبيان باكأب أداة سهلة الاستخدام يمكن ضبطها لتعمل تلقائيا دوريا ولتضمين الملفات والأدلة التي تحددها وفق معايير اختيار منها شرط أن تكون تغيَّرت منذ آخر مرة، كما يمكنها **ضغط** و**تعمية** المحفوظات.

دليل عملي: ابدأ مع دليل كوبيان باكأب

و يفضل استخدام أداة خاصة بالتعمية مثل تروكريت لحماية ملفات المحفوظات. راجع فصل ٤: "حفظ سرية البيانات الحساسة" لمزيد من المعلومات.

دليل عملي: ابدأ مع دليل تروكريت

النصائح التالية تساعد على انسياب نظام الحفظ الاحتياطي :

- نظِّم الملفات في حاسوبك، بتجميع كل الملفات والأدلة التي تحوي وثائق رقمية بحيث تكون تحت دليل أبٍ واحد، مثل دليل "مستنداتي" في نظم وندوز.
- إن كنت تستخدم تطبيقات تحفظ بيانات في قواعد بيانات خاصة بها فتعرَّف على مواضع تلك الملفات وأسمائها، فإن لم تكن المواضع المبدئية ملائمة فانظر إن كان التطبيق يسمح بتغيير موضعها، وانقلها إن أمكن إلى موضع ما في الدليل الذي يحوي باقي الوثائق.
- أنشئ جدولا زمنيا دوريا للحفظ الاحتياطي.
- حاول وضع إجراءات واضحة مكتوبة لكل العاملين في المنظمة لإجراء الحفظ الاحتياطي، ووضِّح لهم أهمية الأمر.
- اختبر إجراءات الحفظ الاحتياطي والاستعادة بكل تفاصيلها للتيقن من قدرتك على تنفيذها عند الحاجة.

إلينا : حسنٌ ؛ لقد أنشأت محفوظة معماة عندما كنت في العمل ووضعتها على قرص مدمج أحتفظ به دُرج مكتبي ذي المفتاح، وكوبيان مُجدول ليُحدِّث المحفوظة بعد بضعة أيام.

نِيكولاي : لكن ماذا إن نشب حريق في المكتب ؟ أو إن استخدمت الموقع للحشد لمظاهرة بيئية كبرى فقد تتحرك السلطات الأمنية وتداهم مقر المنظمة وتصادر الحواسيب والأقراص والملفات الورقية ؟ أشك أن يمنعهم قفل دُرج المكتب. من الأفضل أن تحفظيها في البيت (إن كان هذا آمنا) أو أن تطلبي من صديق أو قريب بعيد عن نشاطك أن يحفظها لك.

قد يبدو إعداد سياسة الحفظ الاحتياطيِّ، وتعلم الأدوات اللازمة لتنفيذها، والالتزام بها شاقا، إلا أن البداية هي أصعب ما في الأمر، وستجد أن إجراء الحفظ الاحتياطي الدوري وتحديث السياسة

أيسر كثيرا من وضعها لأول مرة. ولأن الحفظ الاحتياطي ربما كان أهم عنصر فيما يتعلق بالأمان الرقمي فستجد في النهاية أن العبء المستغرق كان مُجديا.

تدارك حذف الملفات غير المقصود

عندما تحذف ملفا في وندوز فإن اسمه يختفي من قائمة الملفات المعروضة أمامك في مدير الملفات إلا أن محتوياته تبقى مسجلة على وسيط التخزين، وذلك بسبب الطريقة التي يعمل بها حفظ البيانات في الحواسيب. حتى بعد أن تُخلى سلة المهملات قد يمكن استرجاع الملفات أو أجزاء منها أو معلومات عنها حتى بعد مضي وقت طويل على محوها، أو حتى بعد انتهاء العمر التشغيلي للوسيط وتلفه، وذلك باستخدام تقنيات وأدوات خاصة، ما بين برمجيات متاحة على الإنترنت، وعتادية يستخدمها المحترفون وجهات البحث الجنائي. طالع فصل ٦: "تدمير البيانات الحسَّاسة" للمزيد عن هذا الموضوع.

و هذه وإن حسبناها ثغرة أمنية في حالات معينة إلا أنها يمكن أن تعمل لصالحك إذ تتيح احتمالا لإمكانية استرجاع الملفات التي تتسرع في حذفها قبل أن تكتشف أنه لا توجد نسخة أخرى منها كما ظننت، أو أن تكتشف أنك لا تزال بحاجة إليها، وهو موقف يتعرض له كل مستخدمي الحواسيب إن عاجلا أم آجلا. كما سبق، توجد برمجيات يمكنها استرجاع الملفات المحذوفة حديثا، ومنها برمجية **مجانية** هي أندليت پلس.

دليل عملي: ابدأ مع دليل أنْدِليت پلَس

تذكَّر أن هذه الأدوات لا تنجح دوما في استرجاع الملفات المحذوفة لأن نظام التشغيل يمكن أن يحفظ بيانات حديثة تخص ملفات أخرى فوق بيانات الملفات المحذوفة أو جزء منها وبهذا تطمسها وتصعب كثيرا استرجاعها. لذا فمن المهم للغاية فور إدراك الحاجة إلى استرجاع ملف محذوف عدم استخدام الحاسوب لأي غرض آخر لتقليل احتمالات أن ينطمس، هذا يعني أيضا أفضلية تنصيب أدوات استرجاع البيانات المحذوفة قبل الحاجة إليها، لأن ملفات البرمجية ذاتها قد تطمس الملفات المرجو استرجاعها ؛ وخطر الانطماس السريع يزيد كلما قلّت المساحة الشاغرة على وسيط التخزين.

كما يمكن تشغيل برمجيات الاسترجاع من وسيط خارجي، قرص مدمج مثلا أو شذرة ذاكرة، وإن كانت الملفات المحذوفة في غاية الأهمية ولتعظيم فُرص استرجاعها يفضل وصل سواقة الأقراص كوسيط ثانوي بحاسوب آخر واستخدامه في الاسترجاع، لأنه توجد صيرورات عديدة يمكنها حتى إن لم يفعل المستخدم أي شيء أن تولِّد وتحفظ بيانات على القرص تطمس البيانات الهامة المحذوفة.

٦
تدمير البيانات الحسَّاسة

٦. تدمير البيانات الحسَّاسة

تناولَت الفصول السابقة عددا من الممارسات والأدوات التي يمكن أن تُعِين على حماية البيانات الهامة، لكن ماذا يكون الحال إن رأيتَ أنك لم تعد بحاجة إلى ملفات معينة ؟ إن أردت على سبيل المثال أن تحتفظ بالمحفوظة المعماة لوثائق قديمة كنسخة أرشيفية وأردت حذف النسخة الأصلية من حاسوب العمل، فكيف السبيل إلى فعل هذا ؟

قد يبدو للوهلة الأولى أن الحل هو **حذف** الملفات غير المرغوب فيها، لكن كما جاء في قسم "تدارك حذف الملفات غير المقصود" فإنه توجد أدوات قد يمكن باستخدامها استرجاع ملفات سبق حذفها، وذلك بسبب الطريقة التي يعمل بها تخزين البيانات على الوسائط الرقمية. وللتيقن من أن البيانات المحذوفة لا يمكن استرجاعها من قبل طرف آخر ينبغي استخدام برمجيات خاصة **تمحوها** محوا آمنا، كمثل مفرمة الأوراق التي توجد في المكتب ؛ أداة مثل إريسر.

حذف البيانات المتقادمة هو أحد استخدامات المحو، لكنك ما أن تدرك ما قد يجده خصم ما من معلومات عن منظمتك ونشاطك في كمّ الملفات التي كنت تظن أنك حذفتها في حين يمكنه استرجاعها، فإن استخدامات أخرى سترد على ذهنك، مثل محو سواقات الأقراص الصلبة المتقادمة قبل التخلص منها، ومحو سجلات نشاط استخدام التطبيقات في الحاسوب، وتأريخ تصفح الوب، والذاكرة المخبئية والملفات المؤقتة. سيكلينر هي الأداة الأخرى المشروحة في هذا الفصل وتساعد في محو الأنواع الثلاثة الأخيرة من البيانات وأنواع أخرى من المعلومات التي تولدها الحواسيب وتحفظها تلقائيا دون تدخُّلٍ من المستخدم.

سيناريو تطبيقي

إلينا ناشطة بيئية في دولة ناطقة بالروسية، وهي تدير موقعا على الوب تزداد شهرته باضطراد لتوثيقه الأنشطة غير المشروعة التي تدمر الغابات في المنطقة، وهي تحتفظ بنسخ احتياطية من محتوى الموقع في منزلها وفي المكتب وعلى حاسوبها المحمول، ومن ضمن هذه المعلومات سجلات الزوار ومداخلاتهم في منتدى الموقع. تنوي إلينا السفر قريبا إلى دولة أخرى لتحضر مؤتمرا للناشطين البيئيين، وقد أبلغها بعضهم أن حواسيبهم قد أخذت عند المعابر الحدودية لمدة تزيد على الساعة وفحصت محتوياتها، ولأجل حماية بياناتها الحسّاسة ولسلامة النشطاء المتداخلين في موقعها فقد وضعت محفوظتها التي في المنزل والمكتب في مجلدات معماة باستخدام تروكريپت وحذفت النسخة على حاسوبها. وهي تستشير ابن أختها نِيكولاي، وقد نبَّهها إلى أن عليها أن تفعل ما يزيد على مجرّد حذف المحفوظة القديمة إن كانت تخشى أن يُفحص حاسوبها عند الحدود أو يصادر.

ما يتناوله هذا الفصل

- محو البيانات الحسّاسة من الحاسوب بحيث لا تُسترجع
- محو البيانات المخزنة على وسائط محمولة مثل الأقراص المدمجة وشذرات الذاكرة

- تقليل قدرة المهاجمين على معرفة معلومات عن الوثائق التي عَمِلتَ عليها مؤخرا على الحاسوب
- محو وسيط التخزين بحيث لا يمكن استرجاع الملفات التي كانت قد حذفت سابقا

مثالب صيرورة حذف البيانات الرقمية

من المنظور التقني البحت لا يوجد **حذف** فعلي للبيانات المخزنة على وسيط رقمي. من الممكن طبعا أن تضغط زر "الحذف" في لوحة المفاتيح أو تسحب وتسقط أيقونة ملف فوق أيقونة سلة المهملات على سطح المكتب، إلا أن ما يُحدثه هذا في الواقع هو إزالة أيقونة الملف غير المطلوب، وإزالة اسم الملف من فهرس الملفات في نظام الملفات الذي ينظم استغلال الوسيط، وبهذا يعلم نظام التشغيل أن الحيز الذي كانت تشغله بيانات الملف على وسيط التخزين قد أصبح شاغرا يمكن لبيانات أخرى أن تشغله أو بعضا منه. وإلى أن يحفظ النظام بيانات أخرى في ذلك الموضع، فإن البيانات العتيقة ستظل قابعة في ذلك الحيز. ولهذا السبب يمكن لمن يحوز المعرفة التقنية والأدوات المطلوبة أن يسترجع ملفات كانت قد حُذِفت كما هو مبين في قسم "تدارك حذف الملفات غير المقصود".

اعلم أن ملفات تحوي بيانات قد تكون دالة على طبيعة عملك وتتضمن معلومات حساسة تُنشأ وتحفظ على السواقة الصلبة التي يعمل منها وندوز، ثم تُحذف تلقائيا أثناء عملك على الحاسوب دون أن يكون لك تدخل مباشر في ذلك، بما في ذلك ملفات تحوي مقاطع من محتوى الملفات التي تعمل على تحريرها. إذا سار كل شيء كما هو متوقع وإن كانت البرمجيات جيدة التصميم فإن تلك الملفات المؤقتة والمرحلية تحذف تلقائيا ولا تتراكم ولا تستنفد حيز التخزين المتاح لك، إلا أنها عندما تحذف فإن حالتها تكون كحالة الملفات المحذوفة يدويا كما هو موضح أعلاه، ومع أنه لا ضرر مباشر من هذه الصيرورة على سلامة الحاسوب، إلا أن وجود بيانات حساسة غير ظاهرة يمكن استعادتها من قبل مُخترقٍ قد يشكل تهديدا أمنيا.

تذَكَّر كذلك أن سوَّاقات الأقراص الصلبة في الحواسيب ليست وسائط التخزين الوحيدة التي تحوي بيانات رقمية حسّاسة، بل توجد أيضا أقراص سي‌دي و دي‌في‌دي و شذرات الذاكرة المستخدمة مع الأجهزة الرقمية بأنواعها والأقراص المرنة، و السواقات المحمولة بأنواعها.

المحو الآمن للبيانات

عندما تستخدم أداة **محوٍ** آمنٍ مثل المزكاة في هذا الفصل فإن ما يحدث حقا هو أن البيانات المراد محوها تطمس بكتابة بيانات أخرى فوقها، وبهذا لا يعود بالإمكان استرجاع البيانات 'الممحوة' ؛ هذا هو الإجراء الذي نشير إليه 'بالمحو الآمن للبيانات'. ومع أن طمس البيانات بهذه الطريقة يُصعِّب جدا استرجاعها، إلا أنه قد يمكن باستخدام تقنيات متقدمة وأجهزة متخصصة مكلفة استرجاع أجزاء منها تتفاوت حسب التقنية والخبرة، وعموما كلما زادت مرات الطمس بتكرار كتابة بيانات بديلة مختلفة قلت للغاية إمكانية استرجاع البيانات المطموسة. توجد أنماط عديدة لبيانات الطمس وتوصيات مختلفة لعدد مرات الطمس.

محو الملفات والمساحة الشاغرة

لضمان زوال البيانات الحسّاسة ينبغي أن نأخذ في الاعتبار إلى جانب محو الملفات محو المساحة الشاغرة على وسيط التخزين التي ربما كانت مشغولة فيما سبق ببيانات حذفت الملفات التي كانت

تحويها لكنها لم تُمحَ، أو التي شغلتها في وقت من الأوقات ملفات مؤقتة ومرحلية أنشأها ثم حذفها النظام تلقائيا دون تدخلنا وربما حَوَت بيانات حساسة أو معلومات عن كيفية استخدام الحاسوب في أداء الأعمال.

إريسر برمجية حرة – مجانية ومفتوحة المصدر – لمحو البيانات يمكن استخدامها بثلاث طرق مختلفة ؛ بمحو الملفات المختارة في مدير الملفات، أو بمحو كل محتويات سلة المهملات، أو بمحو المساحة الشاغرة على السواقة ؛ كما يمكن باستخدام إريسر محو محتوى **ملف مبادلة** وندوز، للأسباب المشروحة لاحقا.

دليل عملي: ابدأ مع دليل إريسر

ينبغي توخي الحذر عند استخدام أدوات المحو، فمع أن هذه الأدوات لن تضر بملف ولا بدليل ما لم تختره بنفسك وتصدر أمرا لمحوه، ومثلها وظيفة محو المساحة الشاغرة، إلا أن هفوات المستخدمين واردة، وهي سبب وجود تسهيلات مثل سلة المهملات، وكذلك "تدارك حذف الملفات غير المقصود"، غير أن أداء أداة المحو وظيفتها بكفاءة يعني عدم جدوى محاولة استرجاع الملفات الممحوة، وهو السبب الذي لأجله تستخدم أصلا ! لتفادي هذا يستحسن وجود محفوظة احتياطية من البيانات قبل المحو.

لاحظ كذلك أن محو الملفات من بعض أنواع الوسائط الحديثة مثل شرائح يوإس‌بي وبطاقات ذاكرة فلاش بالطريقة المشروحة أعلاه قد لا يكون بذات الوثوقية بسبب اعتماد تلك **النبائط** تقنيات الهدف منها إطالة العمر التشغيلي للنبيطة التخزينية ككل بتبديل المواقع المادية التي تحفظ فيها البيانات على الوسيط بشفافية ودون تدخل من المستخدم ودون أن تتأثر التطبيقات التي تستخدم الوسيط، وذلك لتوزيع البلى عليها بالتساوي. بعض طرز تلك النبائط تحوي وظائف محو مُضمَّنة في العتاد يمكن استخدامها ؛ أو محو المساحة الشاغرة فيها دوريا باستخدام الأدوات المذكورة هنا.

إلينا : أدرك أن تطبيقات معالجة الكلمات مثل ميكروسوفت ورد وأوبن‌أُفِس تحفظ أحيانا نسخا مؤقتة من ملف الوثيقة التي أعمل عليها، فهل تفعل ذلك تطبيقات أخرى ؟ أم يكفني الانشغال بشأن الملفات التي أنشئها وأمحوها بنفسي ؟

نيكولاي : الحقيقة أنه توجد مواضع عديدة في الحاسوب تترك فيها التطبيقات آثارا يمكن اقتفاؤها من المعلومات الخاصة وبيانات تصفح الإنترنت وما شابه، مثل عناوين المواقع التي زرتها، ومتون رسائل البريد التي قرأتها أو أرسلتها.

محو البيانات المؤقتة

الأسلوب والبرمجية السالف بيانهما لا تفيدان في محو البيانات غير المحذوفة التي لا تعرف أنت موضعها لأنها محفوظة في مواضع عديدة في النظام لا يتعامل المستخدم معها عادة، أو بأسماء لا تدل

على شيء مفهوم للمستخدم، أو مدفونة في أدلة عميقة، وجلُّها ملفات ينشؤها النظام والتطبيقات تلقائيا كجزء من عملها، يمكن تعطيل توليد بعضها من تحكمات التطبيقات، إلا أن بعضها الآخر لا يمكن تعطيل توليده. من أمثلة هذه البيانات :

- بيانات يحفظها متصفح الوب أثناء استخدامه، من ذاكرة مخبئية تحوي مكونات الصفحات التي تطالعها من نصوص وصور وفيدوات ؛ وكذلك **الكوكيز**، والبيانات التي يُدخلها المستخدم في الاستمارات وتحفظها المتصفحات للتسهيل، بما في ذلك بيانات الولوج للحسابات، وتأريخ التصفح الذي يسجل المواقع التي زرتها والملفات التي نزلتها.
- ملفات مؤقتة تحفظها التطبيقات المختلفة بمثابة مسودات تحسبا لانهيار النظام أو التطبيق قبل أن يحفظ المستخدم نتيجة أعماله لتمكينه من استعادة أكبر قدر من عمله عندما يعيد تشغيلها. هذه الملفات تحوي نسخا كاملة من الوثائق التي يعمل عليها المستخدم.
- بيانات يحفظها وندوز للتسهيل على المستخدم، مثل اختصارات التطبيقات التي استخدمت مؤخرا واختصارات الوثائق التي عمل عليها المستخدم، وأسماء الأدلة والملفات التي فتحها في التطبيقات، وكذلك محتويات سلة المهملات.
- **ملف مبادلة** وندوز يحوي نسخا من محتوى الذاكرة التي تستخدمها التطبيقات بما فيها متون الوثائق وقد يحوي كلمات السر ومفاتيح التعمية، وهو يبقى محفوظا على القرص الصلب حتى بعد إطفاء النظام.

لإزالة الملفات المؤقتة الشائعة والبيانات الأخرى المذكورة أعلاه يمكنك استخدام أداة مجانية مثل سيكلينر المصمم بغرض التنظيف خلف تطبيقات مثل متصفحات الإنترنت إكسبلورر وفيرفكس، وتطبيقات ميكروسوفت أوفس، وجميعها معروفة بأنها تترك آثارا يمكن اقتفاؤها من البيانات الحسّاسة. يعرف سيكلينر مواضع حفظ الملفات المطلوب **محوها** محوا آمنا مما يقلل الحاجة إلى محو المساحة الشاغرة باستخدام أداة أخرى مثل إريسر فيما لو كان سيكلينر طبق الحذف العادي.

دليل عملي: ابدأ مع دليل سيكلينر

ملاحظة : في وقت كتابة هذا الدليل فإن الإصدارة الأحدث من أداة التعمية تروكريت بوسعها تعمية سواقة النظام بكاملها بحيث يعمل النظام بأكمله ببياناته وتطبيقاته في حاوية معماة تمنع تسرُّب أي بيانات من المذكورة أعلاه عند إطفاء النظام وقفل المجلد كحلٍّ بديل آمن. هذه الوظيفة غير مشروحة في دليل استخدام تروكريت في هذه الإصدارة من العدة.

نصائح للمحو الآمن للملفات

بينت الأقسام السابقة الكيفية التي يمكن أن تنكشف بها البيانات على الحاسوب أو وسيط التخزين، كما بينت الأدوات التي يمكن باستخدامها **محو** البيانات بما يحول دون استرجاعها.

للتيقن من إزالة آثار البيانات الحساسة من السوَّاقات يُنصح باتِّباع الخطوات التالية، خصوصا إن كنت تشرع للمرة الأولى في استخدام تلك الأدوات :

١. احفظ نسخة احتياطية مُعمّاة من البيانات المحفوظة على الحاسوب، كما هو مبين في فصل ٥: "تَدارُكُ فَقْدِ البيانات".
٢. أغلق كل التطبيقات غير الضرورية وافصل الحاسوب عن الإنترنت.
٣. امحُ كل الملفات غير الضرورية من كل وسائط التخزين الموصولة، وأخلِ سلة المهملات.
٤. امحُ الملفات المؤقتة باستخدام سيكلينر.
٥. امحُ **ملف تبادل** وندوز باستخدام إريسر.
٦. امحُ المساحة الشاغرة على وسيط التخزين باستخدام إريسر. هذه الخطوة قد تستغرق وقتا طويلا وتبطئ استخدام الحاسوب، لذا فقد تريد بدء هذه الخطوة في نهاية اليوم وتركها تعمل طوال الليل.

إن كانت سعة السواقة الصلبة كبيرة والحجم الذي تشغله الملفات غير الضرورية – التي تنوي حذفها – ومعها محتويات سلة المهملات كبيرا فيمكن تقديم الخطوة الأخيرة لتصبح الثالثة لتوفير بعض الوقت.

اعتد أن تفعل التالي بانتظام :

- استخدام سيكلينر بانتظام لمحو الملفات المؤقتة محو ملفات العمل غير المرغوبة باستخدام إريسر عوضا عن الحذف التقليدي، ومحو محتويات سلة المهملات.
- استخدام إريسر دوريا لمحو المساحة الشاغرة على مشغلات الأقراص وشذرات يوإسبي ووسائط التخزين الأخرى التي قد تحوي بيانات حساسة، مثل الأقراص المرنة وذواكر أجهزة التسجيل الصوتي وبطاقات ذاكرة الكاميرات الرقمية.

نصائح لمحو كل محتويات وسائط التخزين

عندما تتقادم سوّاقة الأقراص الصلبة أو الحاسوب كله، أو عندما تشتري آخر أحدث وأكبر وتعتزم التخلص من العتاد العتيق ببيعه أو إهداءه لشخص ما أو التبرع به لمدرسة أو منظمة أهلية، فينبغي عندها **محو** محتوى السوّاقة بكاملها باستخدام أداة للمحو الآمن مثل إريسر.

أيضا إن تعطلت السواقة أو انهارت فجأة واستبدلتها بأخرى، أو إن قررت التخلص من العتيقة – سواء كانت تعمل أو تالفة – بإرسالها إلى جهة تدور مكوناتها أو تتخلص منها بطريقة آمنة لا تلوث البيئة، وذلك بدلا من إعطائها لمن يستخدمها فيفضل إتلاف السواقة ماديا بتحطيمها، لأن السواقات المعطوبة قد يتمكن خصم ذو دراية تقنية من استخراج معلومات منها حتى لو لم تستطع أنت تشغيلها لاستخدامها. المدى الذي تذهب إليه في هذا الشأن، مثل كل إجراءات تدمير البيانات الأخرى، يتوقف على مدى حساسية البيانات وعلى مدى الجهد والتكلفة التي قد يبذلها الخصم المتوقع لاستخراج المعلومات والعزم الذي يُتوقع أن يبديه.

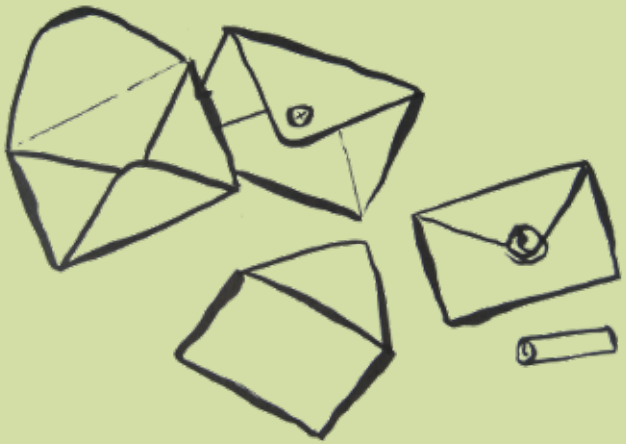
في كل من الحالات المذكورة أعلاه ينبغي طبعا أن تنسخ محتويات السواقة العتيقة إلى الجديدة، أو أن تسترجع البيانات من محفوظة احتياطية إلى السواقة الجديدة، بعدها يمكن وصل السواقة العتيقة بحاسوب كسواقة داخلية ثانوية أو كسواقة خارجية بوصلة يوإسبي ومحوها باستخدام إريسر، وذلك بأن تمحو كل الملفات والأدلة ثم أن تمحو المساحة الشاغرة باستخدام عدد مرات محو مناسب.

الوسائط التي لا يمكن محوها مثل الأقراص المدمجة ؛ سي‌دي و دي‌في‌دي تنبغي معاملتها مثل الأوراق ؛ بإتلافها، و يمكن قبل ذلك نسخ البيانات التي لا تزال صالحة و ضرورية من القرص قبل إتلافه. و بالرغم من أن الأقراص المخدوشة قد يستصعب استخدامها على الشخص العادي، إلا أن الأقراص المدمجة في الحقيقة يصعب تدميرها، و قد تكون قد سمعت حكايات عن البيانات التي استرجعت من أقراص كُسرت إلى قطع صغيرة، لكن تذكَّر أن هذا صعب جدا و يتطلب خبرة كبيرة، و هنا كذلك عليك إعمال العقل في مدى فداحة التهديد الذي قد تتعرض إليه و مدى عزم المهاجم و أن تأخذ في الاعتبار التكلفة و السهولة النسبية لوسائل أخرى قد يلجأ إليها للحصول على المعلومات. لكن عموما يمكنك تدمير الأقراص بمقص أو مفرمة أوراق قوية أو مفرمة خاصة للأقراص و أن تخلط شظاياها و تتخلص منها في مقالب نفايات مختلفة بعيدة عن المنزل و المكتب.

إلينا : لا يزال لديّ قرص مدمج عليه محفوظة عتيقة من سجلّ خادوم الوب، و قد سمعت أنه من الممكن محو محتوى القرص المدمج بوضعه في فرن الميكرويف، إلا أنها بدت لي فكرة سيئة. هل ينفع هذا حقا ؟

نيكولاي : أتخيل أن هذا يُدمِّر البيانات بفعالية، لكني لا أعرف يقينا لأني لم أضع قرصا مدمجا في الميكرويف من قبل، و معك حق في أنها لا تبدو فكرة جيدة. فحتى لو لم يخرب الفرن أو يتسبب هذا في حريق، فأتخيل أن اللدائن المنصهرة ستخرج أبخرة ضارة، لذا فلا أوصي حتى بحرق الأقراص بأي كيفية أخرى.

٧
حفظ خصوصية الاتصالات عبر الإنترنت



٧. حفظ خصوصية الاتصالات عبر الإنترنت

إن سهولة ورخص تكلفة التراسل بالبريد الإلكتروني وتقنيات الدردشة والتحاور اللحظي الأخرى تجعلها قيمة للغاية للأفراد والمنظمات، حتى لأولئك الذين ليس لديهم سوى اتصال محدود للغاية بالإنترنت. أما الذين لديهم اتصال أسرع فإن لأدوات الاتصال الصوتي مثل سكايب (Skype) وغيرها من تقنيات VoIP عندهم قيمة بالغة كذلك. لكن استخدام تلك الوسائل الرقمية للتواصل بما يحفظ خصوصية المراسلات وسرية البيانات الحساسة يتطلب تعلّم ممارسات واستخدام أدوات إضافية، وهذا ليس جديدا ولا يختلف عن وسائل الاتصال التقليدية، فالبريد التقليدي والهاتف التقليدي كلها معرضة للأخطار ذاتها، خاصة عندما يستخدمها أشخاص مستهدفون.

علاوة على هذا فاستخدام الوسائل الرقمية يزيد من المخاطر بدرجة أكبر من استخدام الوسائل التقليدية، وذلك لطبيعتها التي تجعل لها ميزة نسبية في الرخص والسرعة، فالرقابة على وسائل الاتصال الرقمية أيضا رخيصة وأكثر كفاءة، حيث يمكن للحواسيب أن تراقب بيسر بالغ قنوات اتصالات عريضة وسريعة يستخدمها عدد كبير جدا من الأشخاص، وتكون لديها بيانات الاتصال كاملة من مرسل ومتلق ومضمون ؛ بينما يتطلب إجراء رقابة بالقدر ذاته من الشمول والكفاءة على قنوات الاتصال التقليدية موارد أكثر بكثير.

مع هذا، فباتخاذ احتياطات معينة يمكن أن ينعكس الحال وتصبح وسائل الاتصال الرقمي أكثر أمنا، فاستخدام **التعمية** القوية يتيح درجات من الخصوصية لم تكن متاحة من قبل سوى لأجهزة الاستخبارات والجيوش الوطنية، وهذا ممكن مع الاحتفاظ بالمرونة التي تتيحها الاتصالات عبر الإنترنت.

الإرشادات المقدمة في هذا الفصل والأدوات المتناولة فيه تعين من يستخدمها على زيادة درجة خصوصية الاتصالات. بريد رَيْزْأب وملحقة OTR لعميل المحادثة الفورية بِدْجِن وموزيلا فَيَرْفُكْس وملحقة إنجْمِيل لعميل البريد ثَنْدَرْبِرْد كلها أدوات جيدة ومفيدة ؛ لكن ينبغي أن تتذكر عند استخدامها أنه ما من وسيلة يمكنها ضمان سرية محادثة ما قطعيا، وأنه يوجد دوما خطر ما لم تحسب له حسابا، سواء كان **مسجل لوحة مفاتيح** مزروع في الحاسوب، أو شخص ما يسترق السمع عند الباب، أو مُراسِل مُهمِل في ممارسات الخصوصية يعرضك معه للخطر، أو شيء غير ذلك.

يهدف هذا الفصل إلى مساعدتك على تقليل تلك المخاطر دون الاضطرار إلى تلافي استخدام وسائل الاتصال عبر الإنترنت في كل ما يتصف بالسرية، وهي توصية البعض.

سيناريو تطبيقي

كلَوديا وپابلو يعملان مع منظمة حقوقية أهلية في بلد في أمريكا الجنوبية، وقد أمضيا أشهرا يجمعان شهادات عيان عن انتهاكات حقوق الإنسان التي ارتكبها الجيش في منطقتهما، وهي شهادات قد يُعرِّض انكشافُها الشهودَ لخطرٍ داهم ومعهم الحقوقيين والناشطين في عدة منظمات تعمل في المنطقة. لذا فقد احتاطا بإجراءات لحماية تلك المعلومات، فهما يحتفظان بالمعلومات الضرورية وحسب مخزنة في مجلد تروكريپت توجد منه عدة نسخ احتياطية في مواضع مختلفة وتحدَّث دوريا. وهما بصدد نشر جوانب من تلك الشهادات في تقرير يُعدَّانه

وقد وجدا أنهما بحاجة إلى مناقشة بعض المسائل مع زملاء لهما في دولة أخرى، ومع أنهم قد اتفقوا على ألا تُذكر أسماء ومواضع الأطراف المتراسلين في هذه النقاشات فإنهما لا يزالان يودَّان أن يطمئنا إلى أن رسائلهم البريدية ومحادثاتهم بهذا الصدد ستكون سريَّة. لذا فقد دعيا إلى اجتماع لمناقشة سبل تأمين الاتصالات وتريد كلَوديا أن تعرف إن كان لدى أي أحد في المكتب تساؤلات.

ما يتناوله هذا الفصل

- مثالب السرية في خدمات البريد على الوب
- إنشاء حساب بريد جديد آمن
- زيادة درجة أمان حساب البريد الحالي
- تأمين خدمة المحادثة الفورية
- كيفية التصرف في حال الشك في اختراق حساب البريد
- الاستيثاق من هوية المتراسلين بالبريد

تأمين البريد الإلكتروني

توجد ممارسات عدة يزيد اتباعها من أمن الاتصالات البريدية، أولها هو التيقن من أن الشخص الوحيد القادر على قراءتها هو المرسل له، وهذا مشروح في قسمي "تأمين بريد الوب من التَّنَصُّت" و"استخدام حساب بريد آمَن". بعد هذه الأساسيات، قد يكون من الحيوي أحيانا التيقن من أن رسائل البريد المتبادلة أرسلها الأشخاص المعنيون وليس أشخاص غيرهم ينتحلون شخصياتهم، وكذلك أن مضمون الرسائل وصل إلى المتلقي كما أرسله المرسل ولم يتم التلاعب فيه، ووسيلة تحقيق ذلك مشروحة في قسم "تعمية واستيثاق رسائل البريد".

يجب أن تعرف ما الذي ينبغي فعله إن شككت في أن حساب بريدك قد اختُرِقَ، وهو ما يتناوله قسم "نصائح للتعامل مع اختراق حسابات البريد".

تذكَّر كذلك أن تأمين البريد لن يفيد إن كان كل ما تكتبه على لوحة المفاتيح تُسجِّله **برمجيات تجسسية** ترسله أولا بأول إلى جهة ما، لذا فمن المهم مطالعة فصل ١: "حماية الحاسوب من البرمجيات الخبيثة ومن المخترقين"، كما أن فصل ٣: "وضع كلمات سر قوية وحفظها" يُعِين في حماية حسابات البريد والتراسل الفوري.

تأمين بريد الوب من التَّنَصُّت

صُمِّمت الإنترنت شبكة مفتوحة تتدفق خلالها المعلومات في صيغة صريحة، لذا فكل ما ينساب عبرها يمكن اعتراضه والاطلاع عليه بسهولة، ولأن الإنترنت هي شبكة الشبكات، شبكة واحدة تمتد في أنحاء العالم تتوزع الخدمات في أطرافها فإن هذا يتيح لعديدين إمكانية الاطلاع على الرسائل. نتناول في هذا الفصل البريد الإلكتروني تحديدا ونستخدمه في الشرح لكن ما يسري على البريد يسري على أي نوع آخر من الرسائل التي تنتقل عبر الشبكة.

مقدم خدمة الاتصال بالإنترنت الذي تستخدمه هو أول محطة تمر عليه رسالة البريد فور أن تبدأ رحلتها من جهة المرسل، وبالمثل فإن مقدم خدمة الاتصال بالبريد الذي يستخدمه المتلقي

هو آخر محطة تمر عليها الرسالة قبل أن تنتهي رحلتها عنده. عادة ما تتم عمليات التنصت في حلقة مقدم خدمة الاتصال بالإنترنت، وما لم تتخذ احتياطات مضادة فإن التنصت على مراسلاتك أو التلاعب بها قد يتم في أي موضع ما بين هتين المحطتين.

بابلو : كنت أتحدث مع واحدة من شركائنا في هذا الموضوع وقد قالت أنها وزملاءها أحيانا ما يلجؤون إلى حفظ رسائل البريد في دليل "المسودات" في حساب بريد إلكتروني يتشاركونه جميعا ويعلمون كلمة سره، ومع أن هذا قد بدا لي غريبا بعض الشيء إلا أني أظن أن هذا قد يحول فعلا دون أن يتمكن أي شخص غيرهم من قراءة الرسائل بما أنهم لا يرسلونها، أليس كذلك ؟

كلَوديا : أبدا، ففي كل مرة تقرأ فيها شيئا ما على الوب، حتى لو كان رسالة محفوظة في مسودات حسابك البريدي فإن محتواه يُجلب عبر الإنترنت من مقدم خدمة البريد إلى حاسوبك، وإلا لما ظهرت على شاشتك، أليس كذلك ؟ الواقع أن من يراقبك عادة لا يراقب رسائل البريد وحسب، بل يراقب كل ما يمر من حاسوبك وإليه، لذا فهذه الطريقة لن تعمل إلا إن كان كل من يستخدم الحساب المشترك يتصل به عبر قناة اتصال مؤمَّنة، وإذا فعلوا ذلك فالأفضل أن يكون لكل منهم حساب يخصه وأن يستخدموا البريد بالأسلوب الطبيعي فيرسلوا الرسائل لتلافي مثالب التشارك في كلمات السر.

يمكن تأمين الاتصال بين حاسوبك والموقع الذي تطالعه أو تستخدم خدمة فيه، وهذا الأسلوب مستخدم، على سبيل المثال، في مواقع التجارة الإلكترونية عند إرسال بيانات بطاقات الائتمان، والتقنية التي تحقق قناة الاتصال الآمنة هذه تسمى بروتوكول أمان طبقة النقل (Transport Layer Security تختصر إلى TLS)، وكذلك التطبيق الأقدم لذات الوظيفة وهو طبقة المقابس الآمنة (Secure Socket Layer التي تختصر إلى SSL). يمكنك معرفة ما إذا كان اتصالك بموقع الوب مؤمنا بالنظر إلى حقل المسار، حيث تبدأ مسارات المواقع المؤمَّنة بمعرف البروتوكول https، ففي الاتصال غير المؤمن يبدو حقل المسار كالتالي :

عند كون الاتصال مؤمنًا **بالتعمية** بأحد البروتوكولين TLS أو SSL فإن حقل المسار يتغير ليبدو كالتالي :

في حالة الاتصال المؤمن يزيد حرف s الزائد على معرف البروتوكول المألوف ليوضح أن قناة الاتصال بين الحاسوب وخادوم الموقع مؤمنة. كما تقدم المتصفحات الحديثة مؤشرات بصرية أخرى لتوضيح حالة الاتصال المؤمَّن، مثل إظهار أيقونة قفل أو مفتاح في إطار نافذة المتصفح تتغير حالتها ما بين الإقفال والفتح، أو تغيير لون شريط المسار.

قناة الاتصال المؤمنة بالتعمية تحول دون استطاعة شخص ما الاطلاع على ما يمر داخلها وبالتالي دون قدرته على التنصت، كما أن كون الاستيثاق جزءا من بروتوكولات الاتصال الآمن المستخدمة يحول دون التلاعب في المحتوى من قبل مهاجم في المنتصف.

علاوة على فائدتها في حماية كلمات السر وبيانات المعاملات المالية فإن الاتصالات المؤمنة بالتعمية والشهادات الرقمية مفيدة في حماية البريد الإلكتروني أثناء انتقاله من الحاسوب إلى الخادوم عبر مقدم خدمة الاتصال. مع هذا فكثير من مقدمي خدمة البريد لا يدعمون الاتصالات الآمنة، وبعضهم يتيحها فقط في لحظة الولوج إلى الحساب أو يتطلب بعضهم تفعيلها صراحة بكتابة مسار موقع الخدمة كاملا مسبوقا بمعرف البروتوكول الآمن https. وعموما ينبغي التأكد من كون الاتصال آمنا قبل الولوج، ويفضل كذلك أن يكون آمنا عند قراءة أو إرسال الرسائل.

يجب أن تنتبه عندما يُظهر المتصفح رسائل متعلقة **بالشهادات الرقمية** عند الاتصال بالمواقع، فقد يعني هذا أن خطبا ما قد طرأ على الاتصال، مثل أن يحاول أحدهم العبث به أو انتحال هوية الموقع بتحويل الاتصال إلى موقع آخر يبدو ظاهريا مماثلا للموقع الذي تريد الاتصال به، لذا يجب قراءة الرسائل بتمعن قبل النقر لصرفها.

لكن لاحظ أنه في بعض البلاد – أو المؤسسات – التي تفرط في الرقابة على الإنترنت قد يتعذّر استخدام بروتوكولات الاتصال الآمن المشروحة هنا إن أُغلِقَت المنافذ الشبكية المطلوبة لاستخدامها، وفي هذه الحالة يتعين إيجاد طرق بديلة للحفاظ على سرية المراسلات، مثل تعمية كل رسالة باستخدام PGP، ربما بطريق ملحقة إنجميل لعميل متصفح البريد ثندربرد المشروحة في فصل في "دليل الأدوات".

إن كنت تنوي الاعتماد على بريد الوب للتراسل بمعلومات حساسة فينبغي أن تستخدم متصفحا موثوقا بقدر الإمكان، مثل فيرفكس وملحقاته.

دليل عملي: ابدأ مع دليل فيرفكس

بابلو : بعض من سيعملون على هذا التقرير معنا يستخدمون بريد ياهو ويستخدم آخرون بريد هُتميل، وأذكر أن أي سمعت من قبل أن تلك الخدمات ليست آمنة بما يكفي، فهل ذلك صحيح ؟

كلَوديا : محتمل، توجد خدمات بريد أخرى يُنصح بها، وسيكون علينا تغيير عادات بعض الزملاء إن أردنا مناقشة موضوع تلك الشهادات بأمان.

استخدام حساب بريد آمَن

لأجل تقليل النفقات يتغاضى بعض مقدمي خدمة البريد الإلكتروني عن توفير الاتصال الآمن بخوادمهم ؛ والبعض الآخر، مثل كل من ياهو وهُتميل، يتيحونها حاليا حصرا في صفحات الولوج

إلى الحسابات، تلك التي يدخل فيها المستخدم اسمه وكلمة السر ليلِج إلى حسابه، ظنا منهم أن حماية كلمة السر من أن يكتشفها متنصت يكفي لحماية حساب المستخدم من الاختراق وأن في ذلك حماية كافية لخصوصيته. قد يكون هذا كافيا لبعض المستخدمين، لكن ليس للكل، في هذه الحالة تكون الرسالة عرضة لأن يقرأ محتواها كل من يتحكم في **نبيطة** شبكة ما بين حاسوب المستخدم وخادوم مقدم الخدمة. كما أن نظم ياهو وهُتميل حاليا تسجل في ترويسة كل رسالة عنوان بروتوكول الإنترنت (IP) المخصص للحاسوب الذي يُستخدَم في التراسل، وهو ما قد يقلل من خصوصية المستخدِم.

كل تلك الممارسات متغيرة مع الوقت وفقا لسياسات كل مقدم خدمة، وحاليا فإن خدمة بريد جوجل المسماة جيميل تتلافى بعض نقاط الضعف تلك، فهي تتيح الاتصال الآمن بالخادوم منذ لحظة الولوج وطوال استخدام الحساب، ما دام المستخدم قد اتصل بالموقع باستخدام المسار https://mail.google.com وعين بنفسه البروتوكول الآمن https كوسيلة الاتصال (لاحظ حرف s في https)، ويوجد حاليا تحكُّم في خيارات الخدمة في حساب المستخدم يمكن منه تفعيل الاتصال الآمن مبدئيا بشكل دائم وبغض النظر عن المسار المستخدم للولوج إلى الحساب، لكن يفضَّل أن تجرب الاتصال الآمن يدويا أولا قبل أن تفعله بشكل دائم لتتأكد من أنه يعمل في البيئة التي تعمل منها إذ قد يستحيل ذلك في بعض الأحيان كما هو مذكور أعلاه.

لكن مع هذا فلبريد جوجل أيضا عيبه فيما يتعلق بالخصوصية إذ يفحص محتوى رسائل البريد بغرض عرض إعلانات يُظن أنها توافق اهتمامات المستخدم ؛ كما أنه مع أن شركة جوجل، على غير سالفتي الذكر، قد قاومت مسبقا محاولات حكومات الحصول على بيانات شخصية تخص المستخدمين، إلا أن له تاريخا من التعاون مع حكومات في تقييد حرية وصول المستخدمين إلى المعلومات. يُفضل أن تطّلع على سياسة الخصوصية لمقدمي الخدمة الذين تستخدمهم، وأن تتابع التغيرات فيها وأن تلم بالمستجدات في ممارساتهم المتعلقة بالخصوصية بقدر الإمكان.

نحثُّك على فتح حساب بريد في رَيزأب إن أمكن، بزيارة https://mail.riseup.net، وهي خدمة تعاونية تتيح خدمات بريد واستضافة للنشطاء في أنحاء العالم الذين يشتركون معهم في مبادئ سياسية وعقد اجتماعي منصوص عليهما في الموقع ويشترط قبولهما كخطوة من صيرورة التسجيل. يتطلب فتح حساب في ريزأب دعوتين من عضوين مسجلين فيه، إن كنت حصلت على نسخة مطبوعة من هذا الدليل فستجد رمزَي دعوتين مرفقين معه.

دليل عملي: ابدأ مع دليل بريد ريزأب

كلا من بريد جيميل ورَيزأب يتيح وسيلة أخرى لاستخدام البريد، غير بريد الوب، فهتان الخدمتان يمكن استخدامهما مع برمجية عميلة للبريد الإلكتروني، مثل ثندربرد، التي تدعم التقنيات التي يتناولها قسم "تعمية واستيثاق البريد الإلكتروني". التأكد من ضبط عميل البريد الإلكتروني ليتصل بالخادوم باتصال مؤمَّنٍ **بالتعمية** له درجة الأهمية ذاتها التي للاتصال بموقع بريد الوب عبر HTTPS. إن كنت تستخدم عميل بريد فطالع دليل استخدام ثندربرد لمزيد من التفاصيل.

تذكَّر أن الاتصال المؤمن يحمي الرسالة أثناء انتقالها ما بين الحاسوب ومقدم خدمة البريد، لكنه لا يحميها أثناء انتقالها ما بين مقدم خدمة البريد الذي يستخدمه المرسل ومقدم الخدمة الذي يستخدمه المستقبل، كما لا يحميها أثناء وجودها على خوادم أي من مقدمَي الخدمة، ولا أثناء حفظها على حاسوب أحد المتراسلين باستخدام عميل بريد. في هذه الحالات قد تكون تعمية الرسالة ذاتها هي ما يفيد في حمايتها.

بابلو : إذن، هل تنصحينني بالتحول إلى استخدام ريزأب، أم هل في وسعي الاستمرار في استخدام جيميل مع التأكد من فتح موقع بريد الوب ببروتوكول *HTTPS* ؟

كلوديا : هذا اختيارك، لكن يوجد ما يجب أخذه في الحسبان عند اختيار مقدم خدمة البريد عموما. أولا، إن كانوا يتيحون الاتصال الآمن بالحساب. جيميل لديها هذا، لذا فلا مشكلة هنا. ثانيا، إن كنت تثق في إدارتهم في أن يحافظوا على سرية مراسلاتك وألا يطالعوها أو يمكنوا الآخرين من الاطلاع عليها. هذا متروك لك. وأخيرا، عليك أن تفكر في ما إذا لم يكن من المناسب أن يُربط ما بينك ومقدم الخدمة ذاك. بكلمات أخرى قد يؤدي بك استخدام عنوان بريد على النطاق *riseup.net* مثلا إلى مشكلات أو يثير الانتباه بسبب شهرته بأن الناشطين يستخدمونه، وفي هذه الحالة قد تفضل بريدا على نطاق شائع وليست له دلالة خاصة مثل *gmail.com*.

أيا كانت أدوات تأمين البريد التي تختار استخدامها فتذكر أن لكل رسالة مرسل وعدد من المتلقين، وانك طرف واحد في الصيرورة الكلية، وأنك حتى لو اتخذت الاحتياطات اللازمة لتأمين مراسلاتك فإن الآخرين قد يسلكون مسالك مختلفة عند التراسل بالبريد. حاول أن تعرف مقدمي خدمة البريد الذين يستخدمهم مراسلوك والقوانين الخاضعين لها، لأنه من الطبيعي أن الدول تتباين في مقدار رقابتها وتدخلها في مراسلات الأفراد. لاحظ أن استخدام كل المتراسلين مقدمَ خدمة مستقل واحد مثل ريزأب يقلل من فرص تعرض المراسلات للرقابة لأن الرسائل لن تخرج عن نطاق شبكة مقدم الخدمة.

نصائح لزيادة خصوصية التراسل بالبريد الإلكتروني :

- اتخذ دواعي الحذر دوما عند فتح المرفقات بالبريد التي لم تكن تتوقعها، أو التي تصلك ممن لا تعرفهم، أو ذات الموضوعات الغامضة. فقبل فتح مرفقات كتلك ينبغي التأكد من أن مضاد الفيروسات مُحدَّثٌ ويعمل وانتبه إلى التحذيرات والرسائل التي تعرضها البرمجيات، المتصفح أو عميل البريد أو مضاد الفيروسات.
- استخدام أدوات التجهيل مثل تور الموصوف في فصل ٨: "الحفاظ على المجهولية وتجاوز الرقابة على الإنترنت" يمكن أن تمنع من يراقب اتصالك بالإنترنت من معرفة خدمة البريد التي تستخدمها، وبناء على درجة الرقابة الموجودة في منطقتك فقد تحتاج إلى استخدام تور أو أحد

أدوات تجاوز الرقابة الأخرى الموصوفة في ذلك الفصل لاستخدام خدمة بريد مثل ريزأب أو جيميل.

- عندما تفتح حسابا تنوي استخدامه بمجهولية لإخفاء هويتك عن مراسليك أو عن قراء المنتديات العامة التي تنشر فيها يجب أن تنتبه إلى ألا تدخل بيانات حقيقة عنك، مثل اسمك. ومن المهم في هذه الحالة أن تتفادى استخدام هُتميل وياهو وغيرهما من مقدمي خدمة البريد الذين يسجلون عنوان آيبي في الرسالة.
- بالأخذ في الاعتبار قدرة آخرين على النفاذ المادي إلى الحاسوب الذي تستخدمه في التراسل فإن إزالة آثار استخدام البريد والتصفح والملفات المؤقتة من الحاسوب قد تكون له أهمية بالغة تضاهي أو تفوق أهمية حماية الرسائل أثناء انتقالها عبر الشبكة. للمزيد عن هذا الموضوع طالع فصل ٦: "تدمير البيانات الحسَّاسة" ودليل استخدام سيكلينر.

نصائح للتعامل مع اختراق حسابات البريد

إن ارتبت في أن أحدا يراقب مراسلاتك فيمكن أن تفتح حساب بريد جديد تستخدمه في مراسلاتك الهامة وتنبه مراسليك إلى أهمية مراسلتك عليه، مع الاحتفاظ بالقديم كتمويه. لكن تذكر أن من تراسلت معهم في السابق قد تكون صناديق بريدهم مراقبة كذلك، لذا ينبغي اتخذا احتياطات إضافية :

- عليك ومراسليك فتح حسابات بريد جديدة والولوج إليها حصرا من أماكن لم تستخدمها من قبل، مثل مقاهي الإنترنت غير التي اعتدت استخدامها، وذلك لتقليل احتمال التعرض إلى الرقابة التي يمكن أن تمارس من خلالها، أو يمكن استخدام إحدى الوسائل المشروحة في فصل ٨: "الحفاظ على المجهولية وتجاوز الرقابة على الإنترنت" لإخفاء اتصالك بمقدم الخدمة البريدية.
- تبادلوا عناوين البريد الجديدة عبر قنوات آمنة، مثل المقابلة الشخصية أو التراسل الفوري أو المحادثة الصوتية المُعمَّيان.
- واصل استخدام صندوق البريد القديم على الأقل لفترة معقولة بقدر لا يثير شكوك المراقب، لكن دون استخدامه في مراسلات حساسة مع الحرص على عدم ظهور أنك تتفادى استخدامه في المراسلات الحساسة. هذا كما يبدو أمر صعب إلى حد ما ويحتاج إلى تركيز.
- صعِّب على الآخرين الربط ما بين شخصيتك الحقيقية وهويتك الجديدة التي فتحت بها حساب البريد الجديد، فلا تتبادل الرسائل ما بين بريدك الجديد والقديم، ولا مع المتراسلين الذين قد يكونون مراقبين.
- تفاد وضع اسمك الحقيقي في بيانات الحساب، وكذلك تفاد وضع عناوين لافتة للرسائل من قبيل "حقوق الإنسان" أو "التعذيب"، اتفق على شفرة مع مراسليك.
- لاحظ أن تأمين البريد الإلكتروني ليست فحواه استخدام وسائل تقنية معقدة بقدر الانتباه إلى الكيفية التي تستخدم بها وسائل الاتصال، وكذلك الانضباط في عادات التواصل الرقمي.

تأمين الاتصال باستخدام وسائل أخرى عبر الإنترنت

مثل البريد الإلكتروني فإن التراسل الفوري (الدردشة) والاتصال الصوتي عبر الإنترنت يمكن أن تكون مؤمَّنة أو غير مؤمَّنة، حسب الأدوات والتقنيات التي تستخدم من خلالها.

تأمين التراسل الفوري

التراسل الفوري، وهو ما يعرف كذلك بالدردشة (أو الشات)، معرض مبدئيا لمخاطر التنصت ذاتها المعرض لها كل ما يمر على الإنترنت من مراسلات. إلا أنه توجد أدوات يمكن باستخدامها تأمين جلسة التراسل، إلا أنه كمثل حالة البريد الإلكتروني تتطلب أن يتخذ كلا الطرفان الإجراءات المناسبة وأن يستخدما البروتوكولات ذاتها.

بِدْجِن برمجية محادثة فورية تدعم أغلب بروتوكولات التراسل الفوري الموجودة، لذا فهي مفيدة حتى في غياب الحاجة إلى تأمين الاتصال إذ أنه يمكن باستخدامها الولوج إلى حسابات التراسل على شبكات عديدة في الوقت ذاته، دون حاجة إلى فتح حسابات جديدة ولا إعادة إنشاء شبكات المعارف. كما أن لكونها **برمجية حرة، مجانية ومفتوحة المصدر** ميزات عديدة منها خلوها من الإعلانات والبرمجيات الخبيثة. ولتأمين جلسات الدردشة توجد ملحقة خاصة تعمل مع بدجن هي OTR (Off-the-record).

دليل عملي: ابدأ مع دليل بدجن

بابلو : بما أن بريد ياهو غير آمن، فهل يعني هذا أن دردشة ياهو غير آمنة كذلك ؟

كلوديا : لو أردنا استخدام التراسل الفوري لنتناقش حول هذا التقرير فمن الأفضل أن نستخدم جميعا بِدجِن مع *OTR*، وعندها يمكننا استخدام خدمة ياهو للتراسل الفوري أو أي خدمة أخرى.

تأمين المحادثات الصوتية

المحادثات الصوتية عبر الإنترنت (Voice Over IP وتختصر VoIP) تُمكِّن مستخدميها من التحدث مع آخرين حول العالم كما لو كانوا يحادثونهم هاتفيا، لكن دون تكلفة إن كانت من حاسوب إلى حاسوب، أو بتكلفة قليلة إن كانت من حاسوب إلى هاتف تقليدي، وهذا يجعلها مفيدة جدا. بعض أشهر برمجيات/خدمات المحادثة الصوتية تتضمن Skype[١] و Gizmo[٢] و Google Talk[٣] و Yahoo Voice[٤] و MSN Messenger[٥].

معظم تلك الخدمات لا تزيد أمنا عن البريد الإلكتروني والدردشة غير المحميان ؛ ووحدهما سكايب وجِزمو تعميان فحوى المحادثة الصوتية، أو حصرا في حالة المحادثة مع مستخدم حاسوب/برمجية آخر وليس إلى هاتف تقليدي ثابت أو محمول. علاوة على ذلك، فإنه بسبب كون البرمجيتين مغلقتي المصدر فإنه يتعذر على الخبراء المحايدين الاطلاع على كيفية تطبيقهما وتقييم مدى حفاظهما على السرية.

إلى جانب المحادثة الصوتية يدعم سكايب التراسل الفوري بالكتابة، وفي حين أن استخدامه في هذا يعد أكثر أمنا من استخدام الوسائل الأخرى دون التعمية التي يوفرها OTR مع بدجن فإن له

عيبين ؛ أولهما أنه لا يمكن استخدامه سوى للدردشة مع مستخدمي سكايب الآخرين، وثانيهما هو المشار إليه سابقا من كونه برمجية مغلقة المصدر لا يمكن معرفة دواخلها. قسم "البرمجيات الحرة" في فصل ١: "حماية الحاسوب من البرمجيات الخبيثة ومن المخترقين" يتناول أفضلية **البرمجيات الحرة**.

تعمية واستيثاق البريد الإلكتروني

الأدوات والمفاهيم المتناولة في هذا القسم موجهة للمستخدمين المتقدمين.

تعمية البريد بالمفتاح العلني

يمكن باستخدام تقنية **التعمية** بالمفتاح العلني إيجاد قدر كبير من الحماية للمراسلات أيا كانت درجة السرية التي يتيحها مقدم الخدمة أثناء نقل الرسائل وتخزينها، وأيا كانت طبيعة قناة الاتصال. بتطبيق هذه التقنية يتحول نص كل رسالة – ومرفقاتها – إلى صيغة لا يمكن لغير المرسل إليه قراءتها، لأن النص المعمى لا يمكن تظهيره إلى النص الصريح مرة أخرى دون حيازة مفتاح. تكمن ميزة هذه التقنية عن تقنية التعمية التناظرية في انتفاء الحاجة إلى تبادل **سر مشترك** قبل إجراء الاتصال ؛ أي لا توجد حاجة لتبادل مفاتيح سرية أو كلمات سر مسبقا، وبهذا تنتفي الحاجة إلى وجود قناة اتصال آمنة.

بابلو : لكن كيف تعمل هذه الطريقة ؟

كلوديا : بالرياضيات. فأنت تعمي الرسالة إلى المرسل إليها باستخدام مفتاحها العلني وهو كما يبدو من اسمه ليس مما ينبغي الحفاظ على سريته، بل يحبذ تداوله ونشره. وعندما تتلقى الرسالة فإنها تستخدم مفتاحها السري الذي لا يحوزه سواها لتظهير الرسالة. وبالمثل، فهي عندما تريد أن تراسلك فإنها تعمي الرسالة لك باستخدام مفتاحك العلني الذي يمكنها أن تحصل عليه من مواضع عدّة أو أن ترسله أنت إليها دون خشية أن يقع في يد غيركما.

يمكن استخدام هذه التقنية مع أي خدمة بريد، لأن الصيرورة تجري على نص الرسالة ذاتها قبل إرسالها ولا تتطلب شيئا من مقدم الخدمة. كما يمكن استخدام التقنية ذاتها لحماية أية بيانات رقمية أثناء تخزينها أو نقلها عبر أي وسيط.

استخدام تقنية **التعمية** هذه قد تجلب الانتباه إلى من يستخدمها، فبينما ينظر إلى تعمية قناة الاتصال التي تستخدم للاتصال الآمن بالمواقع ببروتوكول https وما شابهه بقدر أقل من الحساسية، فإن التعمية بالمفتاح العلني قد تثير شكوكا. في بعض القضاءات التي يُجرَّمُ فيها استخدام التعمية فإن رسالة معماة تُلتقط أثناء إرسالها قد تتسبب في إدانة مرسلها حتى لو تعذر معرفة فحواها. ففي بعض الأحيان نضطر إلى الموازنة ما بين ضمان الخصوصية والبقاء دون مستوى الشبهات. يمكن باستخدام لأساليب الحفاظ على المجهولية أثناء التراسل عبر الإنترنت التقليل من هذا الخطر، كما يمكن بتقنيات **الأستگانوگرافيا** إخفاء حقيقة استخدام التعمية.

تعمية و استيثاق رسائل البريد

التعمية بالمفتاح العلني تبدو معقدة للوهلة الأولى، إلا أنها تسهل بعد فهم الأساسيات، كما أن أدواتها ليست بالغة الصعوبة. ومع هذا فمن المهم فهم الإطار الذي تعمل فيه لتلافي الأخطاء التي تقلل كثيرا من فائدتها أو تمنح إحساسا زائفا بالأمان. توجد لعميل البريد ثَندَربِرد ملحقة هي إنجميل (Enigmail) يمكن استخدامها لتطبيق تقنية التعمية بالمفتاح العلني بنظام PGP.

دليل عملي: ابدأ مع دليل ثندربرد

الاستيثاق من صحة وأصالة المراسلات البريدية عنصر هام للغاية عند التراسل عبر الإنترنت، إذ أن كل من لديه اتصال بالإنترنت ودراية كافية بكيفية عملها يمكنه أن ينتحل شخصيتك أو يرسل إلى آخرين رسائل تبدو كأنها صادرة عنك وعليها عنوان بريدك الإلكتروني، كما يمكنه كذلك خداعهم ليردوا على مراسلاته ليتلقاها هو. كما يمكن لمن لديه سيطرة على جزء من مسار المراسلات التلاعب في فحواها وتغييره بحيث يخدم أغراضه هو، قبل أن يمرره في الاتجاهين إلى المتراسلين الغافلين عن هذا التلاعب ؛ ويمكن لهذا النوع من الهجومات أن يحدث في الوقت الحقيقي، أي مثلا أثناء جلسة تراسل فوري، دون أن يبدو منه شيء لطرفي التراسل الأصليين.

و في هذا ما يدعو إلى القلق من التبعات الخطيرة على الغافلين عن هذا الانتحال، وعلى سَير الأعمال. خاصة أن المتراسلين عبر الإنترنت يفتقدون عوامل كانت في سياقات الاتصال التقليدية تساعد على التقليل من مخاطر الانتحال، مثل الصوت والخط وأمارات الاستيثاق التقليدية الأخرى.

للتقليل من المخاطر السابق ذكرها تستخدم تقنية **التوقيع الرقمي** وهي المبنية بدورها على التعمية بالمفتاح العلني. فبينما تحقق التعمية غرض 'السرية'، فإن التوقيع الرقمي يحقق أغراض 'الاستيثاق' و'الصحة'، إضافة إلى 'الإلزام' في حال وجود رابط ما بين المفتاح وهوية صاحبه.

قسم استخدام إنجميل مع ثندبرد يتناول هذا.

بابلو : لقد حدث من قبل وأخبرني معارف أنهم تلقوا مني رسائل أعلم أني لم أرسلها ! وقد وجدنا وقتذاك أنه محض سُخام، إلا أنني الآن أتخيل مدى الضرر الذي كان يمكن أن يحدثه ذلك لو كانت الرسالة تحوي معلومات تتعلق بنا أو بعملنا. وقد سمعت أنه بالإمكان تفادي ذلك باستخدام التوقيع الرقمي، لكن ما هو وكيف يعمل ؟

كلوديا : التوقيع الرقمي مثل التوقيع التقليدي بخط اليد وختم الشمع، باستثناء أنه لا يمكن تزييفه. فهو يفيد في التحقق من إذا ما كان المرسل هو حقا من يدعيه وإن كانت فحوى الرسالة قد جرى التلاعب بها من عدمه.

روابط إلى الوب

[١] http://skype.com
[٢] http://gizmoproject.com
[٣] http://google.com/talk
[٤] http://voice.yahoo.com
[٥] http://get.live.com/messenger

٨
الحفاظ على المجهولية وتجاوز الرقابة على الإنترنت

٨. الحفاظ على المجهولية وتجاوز الرقابة على الإنترنت

توظف دول عديدة أنظمة للتحكم في ما يمكن لمواطنيها النفاذ إليه من مواقع ومطالعته من محتوى منشور على الإنترنت، كما أن مؤسسات الأعمال والمدارس والجامعات والمكتبات العامة تستخدم أحيانا أنظمة مشابهة لمنع نفاذ روادها إلى ما تراه إداراتها غير مناسب لطبيعتها ونظمها أو غير متوافقة مع أهدافها، أو لترشيد استخدام مواردها الشبكية والحاسوبية وانتباه موظفيها وقصرها على الأغراض التي تعنيها. تتنوع طرق إنفاذ هذه الرقابة على محتوى الإنترنت، فبعض النظم تتحكم بطريق مراقبة عناوين الإنترنت للمواقع المطلوب النفاذ إليها فتمنع النفاذ إلى المدرج منها في قوائم سوداء، بينما تحوي القوائم السوداء لبعضها الآخر أسماء نطاقات أو مسارات صفحات وملفات محددة، كما تنظر بعض النظم في المحتوى المطلوب بحثا عن كلمات بعينها مدرجة في قوائم وتمنع النفاذ إلى كل ما يحوي تلك الكلمات أو توافيق منها، ويوظف بعضها توليفات من تلك الأساليب في الآن ذاته.

في أغلب الأحيان يمكن تجاوز الرقابة باستخدام التعمية أو التمويه لإخفاء المحتوى، أو الخواديم الوسيطة أو بالمزاوجة بينهما. **الخادوم الوسيط** (بروكسي) هو خادوم خارج بلدك، وهو بالتالي لا يتأثر بالرقابة المفروضة عليك، ينوب عنك في طلب المحتوى ثم تمريره إليك، وكل ذلك بشفافية لا تؤثر بعد إعدادها على كيفية الإبحار على الشبكة. توجد أنواع عديدة من الخواديم الوسيطة توظف توافيق من تقنيات مختلفة، ويتناول هذا الفصل بإيجاز شبكات المجهولية عديدة الخواديم الوسيطة، يليها تناول أكثر تفصيلا للخواديم الوسيطة البسيطة.

سيناريو تطبيقي

منصور وماجدة شقيقان من بلد عربي لديهما مدونة ينشران فيها دون إفصاح عن هويتهما عن انتهاكات حقوق الإنسان ويحرضان على التغيير السياسي. لم تتمكن السلطات في بلدهما من إغلاق موقعهما لأنه مستضاف لدى مقدم خدمة خارج الدولة، إلا أنها سعت إلى معرفة هوية القائمين على الموقع بمراقبة نشاطهم عليه. منصور وماجدة قلقان من أن تتمكن السلطات من متابعة نمط تحديثاتهما للموقع واستنتاج هويتهما استنادا إلى معلومات يتيحها للسلطات مقدمُ الخدمة على نحو غير قانوني، كما أنهما يريدان الاستعداد ليوم تحجب السلطات موقعهما، وذلك ليتمكنا من مواصلة النشر عليه وكذلك لتعريف مواطنيهما بأسلوب تجاوز الرقابة لمواصلة مطالعة الموقع.

ما يتناوله هذا الفصل

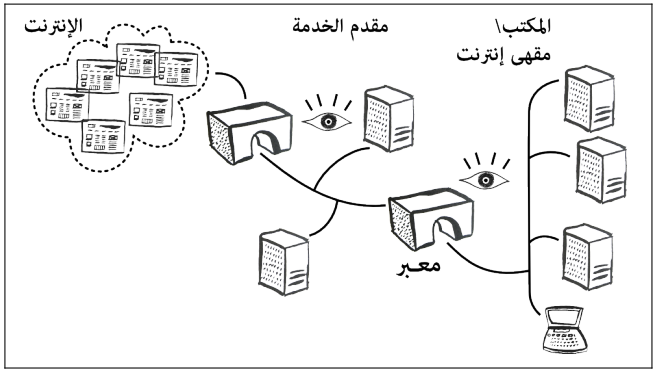
- النفاذ إلى مواقع الوب المحجوبة في بلدك
- الحول دون معرفة المواقع التي تزورها معلومات عن موقعك الجغرافي
- الحول دون معرفة مقدم خدمة الاتصال بالإنترنت الذي تستخدمه أو الجهة التي تمارس الرقابة معلومات عن نمط استخدامك للإنترنت والمواقع التي تزورها

فهم الحجب على الإنترنت

الأبحاث التي تجريها مؤسسات مثل OpenNet Initiative[١] ومراسلون بلا حدود[٢] تبين أن دولا عديدة تحجب أنواعا من المحتوى الاجتماعي والسياسي وما تعده يمس "الأمن القومي" لتلك الدول، وذلك دون نشر قوائم محددة للمحتوى المحجوب. وطبيعي أن الدول التي تُعنَى بالتحكم في نفاذ مواطنيها إلى الإنترنت تتخذ من الإجراءات ما يحول دون نفاذهم إلى الخواديم الوسيطة المعروفة والمواقع التي تقدم أدوات وإرشادات إلى كيفية تجاوز الحجب والرقابة.

بالرغم من صراحة المادة ١٩ من الإعلان العالمي لحقوق الإنسان[٣] في النص على حق كل إنسان في «استقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت» فإن عدد الدول الممارسة للحجب والرقابة على الإنترنت تواصلت زيادته عبر السنوات الماضية، ومع انتشار ممارسة مراقبة الإنترنت زادت أدوات تجاوزها وعدد المهتمين بتطويرها وتحسينها من المبرمجين والناشطين والمتطوعين.

قبل مواصلة استكشاف وسائل تجاوز الرقابة على الإنترنت ينبغي فهم كيفية عمل الرقابة، وفي سبيل ذلك يمكننا تخيل مبسط للإنترنت ولكيفية الاتصال بها.



الاتصال بالإنترنت

عادة ما نتصل بالإنترنت في المنزل أو العمل أو المدرسة أو مقهى الإنترنت عبر مقدم خدمة اتصال، يخصص مقدم الخدمة للحاسوب عنوان الإنترنت فريد يستخدم لتمرير البيانات بين الحواسيب، مثل صفحات الوب التي تطالعها أو رسائل البريد التي ترسلها وتتلقاها، ولأن توزيع عناوين الإنترنت مرتبط بالأقاليم الجغرافية فإن كل من يعرف عنوان آيبي يمكنه استنتاج موقعك الجغرافي بدقة معقولة، إلا أن موفر الخدمة لديه من البيانات ما يمكنه – وكل من تتاح له تلك المعلومات – معرفة العنوان الذي تتصل منه بدقة كاملة، بسبب طبيعة شبكة الاتصالات.

- **مقدم خدمة الاتصال** سيعلم عنوانك، كما سيعرف الخط الهاتفي الذي تستخدمه في الاتصال بالإنترنت إن كنت تستخدم هذا النمط من الاتصال.
- **مدير مقهى الإنترنت أو مدير الشبكة في العمل أو الجامعة** سيعلم أي حاسوب تستخدم وموضع ذلك الحاسوب وأي **نبيطة** شبكية، مثلا المنفذ اللاسلكي، الذي تتصل به.
- **الجهات الحكومية** قد تعلم كل ما سبق عن طريق الجهات أعلاه، أو مباشرة إن كانت تقوم بدور مقدم الخدمة بنفسها.

في هذه المرحلة يعتمد مقدم الخدمة على بنية الاتصال القائمة لتوصيل عملائه بباقي العالم، وفي بعض الدول تستخدم شبكات التلفزة أو شبكات مخصصة للإنترنت. على الطرف الآخر من الاتصال يوجد موقع الإنترنت وقد اتصل بكيفية مشابهة للموصوفة أعلاه عبر مقدم الخدمة الذي يستخدمه، وقد يمر الاتصال عبر عدد من المراحل الوسيطة في أقاليم أو بلدان وشبكات تقع ما بين طرفي الاتصال، وهي تشكل في مجملها الإنترنت، شبكة الشبكات. دون دخول في تفاصيل تقنية فإن هذا النموذج المبسط مفيد في فهم بنية الإنترنت.

حجب المواقع

تتلخص صيرورة الاتصال بموقع ما في طلب يرسله الحاسوب الذي تستخدمه إلى **نبائط** الشبكة لدى مقدم الخدمة طالبا إيصاله إلى خادوم الموقع المطلوب المعرَّف بعنوان الإنترنت المخصص له من قبل مقدم الخدمة إليه. في حال كون الاتصال بالإنترنت غير مراقب فإن مقدم الخدمة سيمرر الطلب عبر عقدة أو أكثر على الشبكة وصولا إلى وجهته، لكن في حال وجود رقابة فإن مقدم الخدمة، ممثلا في أجهزته الشبكية التي يتصل حاسوب المستخدم بها، يسعى لمطابقة عنوان الخادوم المطلوب بمدرجات القائمة السوداء قبل أن تقرر ما إن كانت ستمرر الطلب أم لا.

في بعض الحالات قد تضطلع جهة مركزية، حكومية أو شبه حكومية، بإجراء الرقابة بدلا من مقدمي الخدمة الذين ينبغي أن تمر كل طلباتهم عبرها. كما أن القوائم السوداء عادة ما تحوي أسماء نطاقات، مثل blogspot.com، بدلا من عناوين الإنترنت، مثل 209.85.165.191. وفي بعض الحالات تَفحصُ برمجياتٌ محتوى الرد الوارد من الخواديم وتقرر بناء عليه ما إن كان النفاذ مسموحا، وذلك بدلا من مراقبة أسماء النطاقات وعناوين الإنترنت.

بعض الجهات التي تمارس الرقابة تمارسها في شفافية، فتعرض للمستخدم رسائل توضح أن المحتوى المطلوب محجوب، أحيانا مع إبداء سبب الحجب، وأحيانا مع وسيلة لإبداء الاعتراض أو جهة للاتصال بها أو مراسلتها، إلا أن بعضها الآخر لا يفعل ذلك، وقد تعرض رسائل أعطال غير صحيحة، مثل أن تدعي أن الموقع غير موجود على الشبكة، أو أن الخادوم لم يستجب للطلب قبل نفاذ المهلة.

و عموما، فمن الأفضل والأيسر تبني منظور يفترض الأسوأ فيما يتعلق بآلية ممارسة الرقابة بدلا من محاولة تشخيص أو تخمين الأسلوب الفعلي، لذا فيمكن افتراض التالي :

- أن الرقابة تمارس بفحص المحتوى
- أن الرقابة تمارس بواسطة مقدم الخدمة

- أن المواقع المحجوبة مدرجة في القوائم السوداء كل من عناوينها وأسماء نطاقاتها
- أنه يحتمل عدم صدق رسائل الأعطال التي تدعي تعذُّر الاتصال

و لأن وسائل تجاوز الحجب الأكثر فعالية يمكن استخدامها بغض النظر عن نوع الرقابة المستخدم فإن الافتراضات المتشائمة تلك لا تضر.

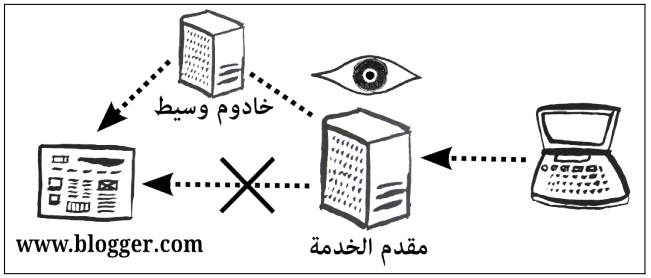
منصور : إذن، ففي اليوم الذي أجدني فيه غير قادر على النفاذ إلى الموقع في حين يمكن لصديق يقيم في دولة أخرى مطالعته دون مشكلة فإن هذا يعني أن الحكومة قد حجبته ؟

ماجدة : ليس بالضرورة، فبعض أعطال الشبكة قد تؤثر على أولئك الذين يحاولون مطالعة الموقع من مكان معين، في هذه الحالة قد تستعين بشخص آخر في منطقتك ذاتها، أو يمكنك أن تجر النفاذ إلى الموقع باستخدام إحدى وسائل تجاوز الحجب وأن ترى إن نجح ذلك.

فهم تجاوز الحجب

إن عجزت عن مطالعة موقع بسبب كونه محجوبا بإحدى الوسائل السابق وصفها فينبغي عليك إيجاد طريق حول ذلك العائق. يمكن **لخادوم وسيط** آمن موجود في بلد لا تمارس الرقابة القيام بهذا الدور عن طريق توجيهه إلى الإنابة عنك في طلب المحتوى الذي تريد ثم تمريره إليك. من وجهة نظر مقدم الخدمة الذي تستخدمه فإنك تقوم بالاتصال الآمن مع حاسوب غير معروف – وغير محجوب – على الشبكة. إلا أن الجهة الحكومية التي تمارس الرقابة أو الشركة التي تجمع وتوفر القوائم السوداء قد تكتشف في النهاية دور ذلك الحاسوب المجهول كوسيط لتفادي الحجب، وعندها فإن عنوانه أو اسم نطاقه قد يضاف بدوره إلى قائمة الحجب ولن يمكن استخدامه بعدها، ومع أن السجال دائر ما بين المستخدمين الذين يبحثون عن وسطاء غير محجوبين وما بين جهات الرقابة التي تستكشف الوسطاء لحجبهم، فإن مطوري نظم تجاوز الرقابة يسلكون أحد المسلكين التاليين أو كليهما :

- **الوسطاء الخفيين** التي لا يعلن عنها يكون اكتشافها أصعب
- **الوسطاء المستهلكين** وهي وسطاء يمكن الاستغناء عنها سريعا فور اكتشافها وتكون دورة حياتها قصيرة تعتمد على نشرها بين من يحتاجونها بأسرع مما تكتشفها وتحجبها السلطات



قي النهاية، طالما كان بوسعك الاتصال بخادوم وسيط تثق فيه لجلب المحتوى الذي تريد فكل ما عليك فعله هو تمرير الطلب إليه باستخدام تطبيق الإنترنت الملائم، تفاصيل ذلك يتولاها تطبيق تجاوز الحجب، أو بتعديل تضبيطات المتصفح أو باستخدام وسيط وب بفتح صفحته في المتصفح. شبكة تور للمجهولية الموصوفة في القسم التالي تستخدم الأسلوب الأول تلقائيا دون تدخل المستخدم.

شبكات المجهولية والخواديم الوسيطة البسيطة

شبكات المجهولية

تمرر شبكات المجهولية تدفقات البيانات المارة عبرها بين عدد من **الخواديم الوسيطة** الآمنة بهدف تمويه مصدرها، ثم لتمويه هدفها، يؤدي هذا إلى إبطاء أدائها بشكل ملحوظ. في حالة تور فإنها تتيح وسيلة عمومية وآمنة لتفادي الرقابة توفر عليك عناء البحث في مسألة ما إن كان ينبغي لك الثقة في مشغلي الخواديم الوسيطة وائتمانهم أم لا. كما نوصي دوما، يجب التحقق من وجود اتصال مؤمن، ببروتوكول HTTPS، قبل تبادل بيانات خاصة مثل البيانات البنكية وكلمات سر الولوج إلى حسابات الخدمات المختلفة.

يلزم تنصيب برمجية خاصة لاستخدام تُور، وهي أداة تحقق كلا من المجهولية وتجاوز الرقابة في آن.

دليل عملي: ابدأ مع دليل تور

يؤدي تُور وظيفة الخادوم الوسيط بأن يحول دون مقدم خدمة الاتصال بالإنترنت ومعرفة الموقع الذي تطلبه، علاوة على ذلك فإنه في كل مرة تُجري فيها اتصالا عبر شبكة تور فإن مسارا مختلفا عبر شبكة خواديم تور يجري إنشاؤه ينتهي بنقطة خروج مختلفة، وهذا يحول دون مقدم المحتوى المطلوب ومعرفة عنوان الإنترنت المخصص لحاسوبك وموقعك الجغرافي، كما تحول التعمية دون اطلاع مقدم خدمة الاتصال على المحتوى الذي تطالعه.

من مميزاته تصميمه المعتمد على فكرة **تسيير البصلة** أنه لا يمكن لكل خادوم وسيط في شبكته أن يعرف سوى الخادوم الذي يليه والذي يسبقه في المسار المؤقت، وبالتالي لا يمكن لأي مشغل عقدة وسيطة أن يستنتج معلومات تقلل من خصوصية المستخدم، ولا أن يطلّع على ما يمر خلال الوسيط الذي يشغله من بيانات تخص المستخدمين، لأنها تَرِدُهُ معماة. يوجد المزيد من التفاصيل عن كيفية عمل تور في دليل استخدامه، والمزيد عن استخداماته الأخرى في الوثائق على موقع المشروع[٤].

من مميزات تور أيضا أنه لا يعمل وحسب مع المتصفح، بل يمكن استخدامه مع أي برمجية تجري اتصالا بالإنترنت، فعملاء البريد الإلكتروني مثل ثُندَربِرد، وعملاء المحادثة الفورية مثل بِدجِن يمكنها العمل من خلال تور بضبطها لاستخدامه كوسيط، إما للنفاذ إلى خدمات محجوبة أو لزيادة المجهولية.

وسطاء تجاوز الحجب البسيطة

توجد ثلاث أسئلة هامة ينبغي أخذها في الاعتبار عند اختيار وسيط بسيط. أولها، ما إذا كان معتمدا على الوب أم أنه يتطلب إحداث تغييرات في تضبيطات البرمجيات أو تنصيب برمجيات جديدة ؛ وثانيهما، ما إن كان آمنا ؛ وثالثهما، ما إن كان عموميا أم خاصا.

وسطاء الوب

وسيط الوب هو موقع على الوب لا يتطلب استخدامه سوى فتح صفحته بمتصفح الوب ثم إدخال المسار المحجوب في الحقل المناسب في الصفحة ثم ضغط زر إرسال الاستمارة، سيجلِب الوسيط الصفحة ويعرضها وكأنها هي جزء من موقعه، ويمكن تتبع الروابط بشكل طبيعي، أو إدخال مسار جديد. لا يتطلب هذا النوع تنصيب برمجيات ولا تغيير تضبيطات.

تتميز وسطاء الوِب بأنها يسرة الاستخدام، وأنه يمكن استخدامها من الأماكن التي لا يسمح فيها بتنصيب برمجيات أو عندما لا تكون مستعدا بالبرمجيات المناسبة، كما أنها آمَنُ نسبيا إن كنت تخشى أن تُضبَط وأنت تستخدم أدوات تجاوز الحجب.

لكن يعيب وسطاء الوب أن بعض المواقع لا تعمل معها، فهي قد لا تعرض كل الوسائط في الصفحة من فيديو وبُرمِجات. كما أنه بالرغم من أن استخدام وسيط يستتبع إبطاء التصفح إلا أن وسطاء الوب العمومية عادة ما يكون الضغط عليها كبيرا مما يزيد من بطئها، كذلك فهي لا تعمل سوى مع صفحات الوب وليس مع أي تطبيقات أو بروتوكولات أخرى، مثل تطبيقات البريد أو المحاثة الفورية للنفاذ إلى خدمة محجوبة.

أنواع الوسطاء الأخرى

أنواع الوسطاء الأخرى تتطلب إما تنصيب برمجيات خاصة أو ضبط عنوان الوسيط في المتصفح أو النظام، في الحالة الأولى فإن الأداة عادة ما ستتيح وسيلة لتفعيل وتعطيل عملها، وبعضها يُبدِّل الوسطاء تلقائيا عند عدم القدرة على الاتصال بكل منها إما بسبب حجبه أو عطبه، أو بهدف زيادة المجهولية. إن تطلب الأمر ضبط المتصفح يدويا فستتوجب معرفة عنوان الوسيط، وتغييره عندما يبطئ إلى حد غير مقبول.

و مع أن هذا النوع قد يكون أصعب استخداما من وسيط الوب فإنه ينجح في عرض الصفحات المعقدة على نحو طبيعي. توجد كذلك أنواع أخرى من الوسطاء، مثل SOCKS وهو بروتوكول خاص بالوسطاء، أو تطبيقات الشبكات الخاصة الافتراضية (VPN) التي يمكن استخدامها لتحويل كل مجري الاتصال بالإنترنت لحاسوب أو شبكة.

الوسطاء الآمنين والوسطاء غير الآمنين

نصف كل وسيط يدعم الاتصالات المعماة بأنه وسيط آمن. ومع أن الوسيط الذي لا يدعم التعمية يظل مفيدا في تجاوز أنواع عديدة من الرقابة، إلا أنه لن يفيد في حال كون الرقابة تطبق بفحص المحتوى. من غير المحبذ استخدام وسطاء غير آمنين للنفاذ إلى مواقع عادة ما نتصل بها باتصالات مؤمنة، مثل حسابات البريد، لأننا في هذه الحالة نكشف بيانات حساسة كانت في الأصل ستكون مُعمَّاة. تنبغي ملاحظة أنه في حالة وسطاء الوب فإنه حتى مع وسيط آمن يُجزَّأ الاتصال ما بين العميل والموقع/الخدمة إلى اتصالين منفصلين كل منهما معمى باستخدام https، يتوسطهما الوسيط

الذي تكون له قدرة قراءة وتعديل المحتوى أثناء مروره خلاله بعد جلبه من مصدره وقبل تمريره إلى وجهته، لذا فعامل الثقة في الوسيط يبقى ذا بال. لكن مع هذا يظل استخدام الوسطاء الآمنين أفضل من وجهة نظر المجهولية وتجاوز الرقابة، خاصة مع توافرهم على الإنترنت.

مثلما هو الحال مع كثير من المواقع والخدمات فإن كلا من طَورَي الاتصال الآمن وغير الآمن قد يكون مدعوما عند الاتصال بصفحة وسيط الوب، لذا يلزم التنبه إلى استخدام الاتصال الآمن بإدخال https كمحدد البروتوكول في حقل المسار في المتصفح عند فتح صفحة الوسيط. أحيانا ما تظهر تنويهات بشأن **الشهادة الرقمية** التي يستخدمها الوسيط لاستيثاق الاتصال الآمن، وذلك لأن تلك الشهادات عادة ما تكون مولدة ذاتيا وغير معتمدة من جهة استيثاق معروفة، مما يضع عبء الاستيثاق من صحة الشهادات ومضاهاة بصماتها مع مدير الخادوم الوسيط على عاتق المستخدم إن كان يرغب في ضمان الحد الأقصى من الأمان، كيفية الاستيثاق مشروحة في "الملحق ج" من دليل استخدام سيفون[٥]. وعموما يفضل تفادي إدخال كلمات سر لحسابات حساسة أو تبادل معلومات سرية عبر أي وسطاء غير موثوق في من يديرونها، ولاحظ أنه في حالة الخواديم الوسيطة البسيطة فإن مشغل الوسيط ستكون لديه القدرة على معرفة موقعك الجغرافي عن طريق عنوان الإنترنت المخصص للحاسوب الذي تستخدمه وكذلك معرفة المواقع التي تطالعها عبر الوسيط الذي يشغله.

معرفة ما إن كان وسيط الوب يدعم الاتصال الآمن سهلة، لكنها قد تتطلب بعض البحث في حالة الأنواع الأخرى من الوسطاء. جميع الوسطاء المزكاة في هذا الفصل تدعم الاتصالات المؤمنَّة.

الوسطاء الخاصة والعمومية

الوسيط العمومي يقبل الاتصالات الواردة من أي شخص، بينما تتطلب الوسطاء الخاصة الولوج بكلمة سر، وفي حين أنه من المفيد وجود وسطاء عمومية متاحة للاستخدام فإنها عادة ما يتزايد الطلب عليها كثيرا مما يبطئها، لذا فمع أن الوسطاء العمومية قد تلقى عناية تضاهي التي تلقاها الخاصة أو تفوقها إلا أن الحِمل الزائد عادة يجعلها أبطأ. أما الوسطاء الخاصة فإنها عادة ما تدار كمشروع خدمي هادف للربح، أو أن حق استخدامها يمنح بصفة شخصية من مديرها إلى من يعرفهم شخصيا أو في محط شبكة من المعارف، لذا فمن الأيسر معرفة دافع تشغيل وسيط خاص، إلا أنه من الخطأ افتراض أن الخواديم الخاصة أكثر موثوقية وأمنا من العمومية لذاك السبب، فالحرص على الربح قد دفع خدمات تجارية إلى كشف بيانات عملائهم في السابق، كما أن جهة ذات نوايا خبيثة قد تدير وسطاء تبدو خاصة لتقليل الشبهات.

يمكن إيجاد خواديم عمومية بالبحث في محركات البحث على الوب بكلمات مفتاحية مثل "public proxy" إلا أنه لا ينبغي الاعتماد والوثوق في الوسطاء المعثور عليهم بهذه الطريقة إلا في أضيق الحدود وعند الاضطرار، أما في غير حالات الضرورة يفضل استخدام وسيط خاص آمن يشغله شخص تعرفه وتثق به، إما شخصيا أو بطريق سمعته، ممن لديهم دافع مساعدة الآخرين والقدرة التقنية على إدارة خادوم وسيط بأمان والحفاظ على خصوصية عملائه. فإن تعذَّر عليك إيجاد شخص أو منظمة موثوق بها بوسعها مساعدتك باستخدام وسيطهم فعليك عندها أن تأخذ في الاعتبار خيار شبكات المجهولية مثل تور المشروح في بداية هذا القسم.

إن كنت تعيش أو – تدير حاسوبا – في نطاق لا تُفرض فيه رقابة قسرية أو حتى فيه الحجب قليل نسبيا فيمكنك مساعدة الآخرين الذين يرزحون تحت وطأة الرقابة الأشد أو الشاملة.

تشغيل خادوم وسيط خاص مثل سيفون وفتح حسابات لمن تعرفهم شخصيا مسألة يسرة ومشروحة في دليل استخدام سيفون[٦]، وهو لا يضيف عبئا كبيرا على مواردك الحاسوبية والشبكية خاصة إن كان لديك اتصال دائم بالإنترنت.

كما يمكنك أن تساهم في دعم شبكة تور :

- إن كنت لا تحتاج أنت نفسك إلى استخدام تور لتجاوز الرقابة فيمكنك أن تنضم إلى مئات المتطوعين بتشغيل خادوم تور على حاسوبك الشخصي وتحويله إلى عقدة في شبكة تور مما يساعد على زيادة سرعتها وفائدتها للآخرين، وهو مشروح في وثائق تور على موقع المشروع[٧].
- إن كنت تستخدم تور لتجاوز الرقابة المفروضة عليك أو للمجهولية فيمكنك أيضا ضبطه بحيث يمرر تدفقات شبكة تور عبر حاسوبك للمساعدة على تحسين أداء الشبكة وزيادة قوتها، وعمل هذا يسر جدا من واجهة التحكم فيداليا المشروحة في فصل استخدام تور من هذا الدليل. لاحظ أن لهذا أثر إيجابي على زيادة مجهوليتك بسبب اختلاط تدفقات نشاط تصفحك بسيل تدفقات الآخرين المعماة.

كما يمكنك دوما التبرع بالمال[٨]، أو التطوع بجهد البرمجة والإبلاغ عن العلات للمشروعات التي تراها مفيدة، أو بتعريف الآخرين بالأدوات.

خواديم وسيطة مُزكَّاة لتجاوز الحجب

فيما يلي بضعة أدوات وخواديم وسيطة تساعد على تجاوز الرقابة والحجب على الإنترنت، تصدر جهات ومبادرات عديدة أدوات جديدة طوال الوقت، كما يجري تحديث الأدوات القائمة أيضا، لذا فعليك متابعة تلك التحديثات إما من خلال موقع عدة الأمان أو مواقع مشروعات الأدوات التي تستخدمها مباشرة.

سيفون٢ نظام خوايم وسيطة خاصة عبر الوب. لاستخدام سيفون٢ تحتاج إلى معرفة مسار الخادوم واسم حساب وكلمة سر. يمكنك أن تحصل على حساب من مستخدم لديه بالفعل حساب أو باستخدام رمز الدعوة المتضمن في الإصدارة المطبوعة من هذا الدليل. طالع دليل استخدام سيفون[٩].

Sesawe Hotspot Shield خادوم وسيط عمومي آمن. يتطلب استخدامه تنزيل البرمجية[١٠] وتنصيبها. الشركة المطورة للبرمجية ومقدمة الخدمة تسعى للكسب من الإعلانات، لذا فستظهر لافتات إعلانية في رأس نوافذ المتصفح عند تصفح مواقع عبر اتصال غير معمّى، تدعي الشركة أنها تحذف سجلات عناوين الإنترنت حواسيب المستخدمين وأنها لا تصل إلى المعلنين، إلا أنه يتعذر التيقن من ذلك. ولأن النظام يعتمد على شبكة خاصة افتراضية فإن كل اتصالك بالإنترنت سيمر عبر خواديمهم طالما أنك تستخدم الخدمة. توجد مزيد من المعلومات على موقع الشركة[١١].

Your-Freedom خادوم خاص يمكن استخدامه مجانا أو الدفع مقابل الخدمة التجارية الأسرع ذات القيود الأقل. يتطلب استخدام الخدمة تنزيل برمجية[١٢] وفتح حساب عبر موقع الخدمة، كما يتطلب ضبط المتصفح ليستخدم الوسيط أثناء الاتصال بالإنترنت، وهو مشروح في موقع سيساوي[١٣].

Peacefire ينشرون قائمة كبيرة بخواديم وب وسيطة بعضها مؤمّن وبعضها لا، ويتطلب الاتصال الآمن بالخواديم إدخال https في حقل المسار في المتصفح. الخواديم المضافة حديثا إلى القائمة يُعلن عنها دوريا في نشرة بريدية.

منصور : عظيم ! إذن فمقدم خدمة الاتصال بالإنترنت لا يمكنه معرفة المحتوى الذي أطالع إن استخدمت خادوما وسيطا، أليس كذلك ؟

ماجدة : طالما استخدمنا خادوما وسيطا آمنا و تمعنّا في تنويهات الشهادات الرقمية التي تطالعنا فهذا صحيح. لاحظ أن الوسطاء غير الآمنين سيمكنونك من تجاوز الرقابة والنفاذ إلى المواقع المحجوبة، إلا أنهم سيمكنون مقدم الخدمة أو مدير الشبكة في المكان الذي تعمل فيه من التلصص على استخدامك للإنترنت، ومطالعة المحتوى معا.

روابط إلى الوب

[١] http://opennet.net
[٢] http://www.rsf.org
[٣] http://www.un.org/arabic/aboutun/humanr.htm
[٤] http://www.torproject.org/documentation.html.en
[٥] https://sesawe.net/Using-psiphon-2.html
[٦] https://sesawe.net/Using-psiphon-2.html
[٧] http://www.torproject.org/docs/tor-doc-relay.html.en
[٨] http://www.torproject.org/volunteer.html.en
[٩] https://sesawe.net/Using-psiphon-2.html
[١٠] https://sesawe.net/Anchor-Free-Hotspot-Shield.html
[١١] http://www.hotspotshield.com
[١٢] http://www.your-freedom.net/index.php?id=3
[١٣] http://sesawe.net/Using-Your-Freedom.html

معجم

معجم

مخترقون	"الهكرة" هم شُطّارٌ لديهم دراية عميقة بالحوسبة والشبكات والبرمجة أو بإحدى مجالاتها، ومهارة في استخدام تقنيات المعلوماتية وقدرة على إيجاد حلول مبتكرة للمشكلات، وليسوا بالضرورة مخربين ولا خارجين على القانون، إلا أنه في هذا السياق يقصد بهم كل من يسعى إلى النفاذ إلى حواسيب أو نظام ليس لديه صلاحية النفاذ إليها أو الاطلاع على معلومات لم يصرح له بالاطلاع عليها، أيا كان غرضهم من وراء ذلك.	**hacker**
برمجيات خبيثة	برمجيات كتبت لتخدم غرض المتحكم فيها بغض النظر عن مصلحة صاحب النظام الذي تصيبه أو تعمل فيه، وتشمل الفيروسات والديدان وأحصنة طروادة والبرمجيات التجسسية وغيرها.	**malware**
برمجيات تجسسية	فئة من البرمجيات الخبيثة، برمجيات صُممت بحيث تنقل إلى من يتحكم فيها بيانات من نظام يخص غيره بلا علم مالك النظام المصاب أو رغبته. قد يكون الدافع إلى ذلك هو الفضول، أو أغراضا أمنية، أو أغراضا تسويقية تجارية ؛ وذلك عادة باستخدام وظائف الاتصالات المتاحة للنظام المصاب. من أمثلة البيانات التي تصمم البرمجيات للحصول عليها : المراسلات، وكلمات السر، والبيانات المالية، وأنماط تصفح الإنترنت واستخدام البرمجيات الأخرى.	**spyware**
برمجية حرة	برمجية مجانية ومفتوحة المصدر ؛ منشورة برخص حرة تسمح لأي شخص باستخدامها ونسخها وتوزيعها مجانيا دون مقابل ودون أن يكون بذلك معتديا على حق مؤلفها أو مخالفا قوانين حماية الملكية الفكرية. كما أنه يمكن لكل من يريد أن يطالع شفرتها المصدرية، كما يمكن لمن لديه الدراية التقنية تعديلها بحيث تناسب استخداماته الخاصة أو أن يحسنها أو يغير من الوظائف التي تؤديها أو يعالج العلات التي قد توجد فيها أو أن يبني عليها برمجيات أخرى، وذلك دون الرجوع إلى المؤلفين الأصليين، وبلا شرط سوى أن ينشر نتيجة عمله بذات الرخصة ليعطي غيره ذات الحقوق التي كان قد حصل عليها (غالبا، وحسب متطلبات كل رخصة).	**FOSS (Free Opensource Software)**
برمجيات مجانية	برمجيات يسمح منتجوها باستخدامها مجانا، لكنهم غالبا لا يتيحون شفرتها المصدرية للآخرين كما أنهم يحتفظون بكامل حقوق الملكية الفكرية عليها، وقد يسمحون بإعادة توزيعها كما هي دون أي تعديل فيها.	**freeware**
جِدار النار	برمجية قد تعمل في واحدة أو أكثر من طبقات النموذج الشبكي تقوم بدور حارس الحدود لنظام الحاسوب أو الشبكة لتراقب وتتحكم في مرور تدفقات	**firewall**

البيانات الواردة والصادرة منه وإليه وفق قواعد يحددها المستخدم مدير النظام. قد تشمل القواعد طبيعة الاتصال واردا أو صادرا، أو الطرف الآخر من الاتصال، أو فحوى الاتصال، أو التطبيق المتصل، أو الوقت، أو هوية المستخدم، أو توافيق من هذه المعايير وغيرها.

مُسيِّر نبيطة أو برمجية في شبكات تسيير الرزم يُمرر الرزم (وحدات الاتصال) بناء على عنوان وجهاتها، ويستخدم لوصل الشبكات المحلية والحواسيب بالإنترنت. يوجد مُسيِّر في أجهزة الوصلات السريعة بالإنترنت (مثل DSL وما شابهها). **router**

نبيطة جهاز (عتاد) يشكل جزءا من منظومة حاسوبية أو شبكية ويؤدي فيها وظيفة محددة، مثل تخزين البيانات أو تمريرها عبر الشبكة أو معالجتها بأي شكل. في بعض الأحيان يمكن أن تكون النبيطة افتراضية، أي مُحاكاة بالبرمجيات بدلا من أن يكون عتادا ماديا، إلا أن المكونات الأخرى في النظام تعاملها بذات البروتوكولات كما لو كانت عتادا ماديا. من أمثلة نبائط التخزين مشغلات الأقراص وشذرات ذواكر يوإسبي، ومن النبائط الشبكية المودمات، وبطاقات شبكة، ومن النبائط البصرية الماسحات وكاميرات الوب. **device**

كود المصدر (أو كود مصدري) هي مجموع التعليمات التي تؤلف برمجية ما والتي يكتبها المُبرمِجُ بناء على منطق تصميمي معين ليأمر الحاسوب بتنفيذ وظائف الحوسبة الأساسية، من إدخال ومعالجة وإخراج وتخزين البيانات، بما يحقق الغرض من البرمجية، وذلك باستخدام واحدة أو أكثر من اللغات البرمجية، وأنماط البرمجة. **sourcecode**

قرص حي قرص مدمج عليه نظام تشغيل يمكن تشغيله بإقلاع القرص مباشرة دون الحاجة إلى تنصيبه أو تغيير تهيئة وإعدادات وتضبيطات الحاسوب، وذلك بشكل مؤقت، ثم العودة إلى الوضع الأصلي بإعادة تشغيل الحاسوب. **LiveCD**

تهديدات مادية كل ما يتهدد البيانات نتيجة أفعال لمن لديهم نفاذ مادي إلي الحواسيب ووسائط التخزين، وكذلك كل الأحداث المادية التي يمكن أن تخرب العتاد مثل الحوادث والكوارث الطبيعية والتخريب المتعمد. **physical threats**

نقطة اتصال لاسلكي نبيطة شبكية تتيح اتصال الحواسيب والأجهزة الشبكية الأخرى في شبكة حاسوبية محلية لاسلكية، وهو قد يكون متصلا بأجهزة أخرى تستخدم كمخارج اتصال بشبكات أخرى أو بالإنترنت. **wireless access point**

عنوان التحكم في النفاذ للوسيط معرف شبه فريد يميز كل نبيطة شبكية ويستخدم لتعريف النبيطة في سياقات الاتصال المختلفة. بطاقات الشبكات و**المسيرات** وغيرها من نبائط **Media Access Control address**

شبكية لكل منها عنوان شبه فريد يوضع فيه عند تصنيعه ولا يمكن تغييره إلا بصعوبة.

نظام الإدخال/الإخراج الأساسي الطبقة الأدنى من البرمجيات في نظام الحاسوب الشخصي الذي تنبني عليه المستويات الأعلى من الوظائف، ويشمل تحكمات تحدد تفعيل أو تعطيل جوانب من الوظائف الأساسية وسلوك العتاد. **BIOS (Basic Input/ Output System)**

التعمية تطبيق حسبانات رياضياتية على البيانات الرقمية لتحويلها من صيغتها الصريحة المقروءة إلى صيغة لا يمكن قراءتها إلى بتظهيرها، أي عكس التعمية، لردِّها إلى صيغتها الأصلية وهو ما يتطلب معلومة سرية، مثل كلمة السر أو المفتاح. توجد خوارزميات عديدة لإجراء حسبانات التعمية، لكنها عموما تنقسم إلى نوعين أساسين : تعمية تناظرية، وتعمية بالمفتاح العلني (غير تناظرية). **encryption**

مصدر التيار غير المنقطع نبائط تتكون من مراكم للطاقة الكهربية ومتحسسات لانقطاع التيار، وهي تُوصَّل ما بين الأجهزة المراد حمايتها من تذبذبات التيار الكهربي والمآخذ الرئيسي فتنشحن مراكمها تلقائيا طالما استمر التيار، وفور تحسسها انقطاع التيار من المأخذ تتولى لحظيا إمداد الطاقة إلى الجهاز المتَّصل بها فلا يتعطل عمله لمدة معينة تعتمد على كم الطاقة المخزنة بالمركم. **Uninterruptable Power Supply**

استگانوگرافيا (إخفاء البيانات) أساليب لتمويه البيانات وإخفاء حقيقة وجودها بحيث لا يعرف المهاجم المحتمل أنها موجودة من الأصل، وتوجد لذلك عدة أساليب وتقنيات. **steganography**

مجلد قسم منطقي في وسيط تخزين يستوعب داخله أقساما منطقية أخرى للبيانات مثل الأدلة (directories) والملفات (files). عادة ما ينشأ المجلد في قسم (partition) على وسيط التخزين، وقد يشغل أكثر من قسم في بعض النظم. لاحظ أن الوثائق المرتبطة بويندوز أصبحت تستخدم "مجلد" كمقابل "directory" خلافا لكل نظم التشغيل الأخرى، وهي ترجمة أقل ملائمة وأكثر التباسا. **volume**

حجية الإنكار عدم قدرة إثبات ادعاء ما (عادة اتهام) على من ينكر، مع عدم القدرة على إثبات نفيه، وهو يفيد في الحالات التي تنطبق فيها القاعدة القانونية الناصة على أن "الشك في صالح المتهم" وأن "البينة على من ادّعى". **plausible deniability**

خادوم مكوِّن يعمل في منظومة ليؤدي وظيفة معينة بالاستجابة لطلبات مكونات أخرى في النظام، ويتواصل معها ببروتوكول معين. قد يكون الخادوم في صورة برمجية أو عتاد. **server**

مَيْز الكثافة النقطية في الصورة الرقمية، سواء المحفوظة في ملف أو التي تستطيع طابعة إنتاجها، أو ماسحة ضوئية رقمنتها، أو كاميرا تسجيلها. وهي إحدى محددات جودة الصورة وتتناسب معها طرديا، ومعها الذاكرة اللازمة لتخزينها. المحدد الآخر لجودة الصور الرقمية هو العمق اللوني. **resolution**

ضغط البيانات هو إجراء حسبانات رياضياتية على البيانات لتحويلها إلى شكل يشغل حيزا أقل عند تخزينها على الوسائط الرقمية أو عند نقلها، ثم يمكن إعادتها إلى صيغتها الأصلية بخوارزميات أخرى. يوجد نوعان رئيسيان من الضغط، أولهما هو **الضغط غير الفقود** الذي يقلل حجم البيانات دون فقد أي قدر منها وبحيث تطابق البيانات بعد إزالة الضغط عنها البيانات الأصلية قبل الضغط ؛ وثانيهما هو **الضغط الفقود** الذي يُفقد أثناء إجرائه قدر ما من البيانات، بهدف تقليل الحجم بدرجة كبيرة، والقدر المفقود يُعدُّ غير مؤثر في إدراك البيانات، وعادة ما يستخدم في ضغط وسائط الصور والصوت والفيديو التي يتوقف تقرير مدى ميزها أو وضوحها على الحواس والإدراك الإنساني. **data compression**

الحذف/ المحو فيما يتعلق بالحواسيب فإن **حذف** الملفات هو إشارة لنظام الملفات الذي ينظم استغلال وسيط التخزين بأن المساحة التي كان يشغلها ملف ما قد أصبحت شاغرة ويمكن استغلالها لاحقا لغرض آخر، وهو يماثل حذف عنوان فصل ورقم صفحته في فهرس كتاب، مع الإبقاء على صفحات الفصل ذاتها في متن الكتاب. **المحو** هو طمس محتوى الملف من بيانات مخزنة على الوسيط الرقمي بطريق كتابة بيانات أخرى فوقها، وهي الطريقة الآمنة لتدمير البيانات وضمان – أو تقليل احتمال – أن يتمكن شخص ما من استرجاعها باستخدام تقنيات متاحة ومعروفة. **deletion vs. wiping**

ملف مبادلة "المبادلة" (swapping) أسلوب تستخدمه نظم التشغيل لزيادة الذاكرة المتاحة لتشغيل تطبيقات المستخدمين باستخدام جزء من ذاكرة التخزين الثانوية المتمثلة في السواقات الصلبة الأبطأ والأكبر للحفظ المؤقت لبعض محتوى الذاكرة الرئيسية المتمثلة في الرام (RAM) التي تعمل فيها التطبيقات والتي عادة ما تكون أقل في السعة إلا أنها أسرع كثيرا، وبهذا يمكن للتطبيقات أن تستخدم قدرا من الذاكرة يفوق ما هو موجود فعلا في النظام. **swap file**

الكوكيز الكوكيز وسيلة تستخدمها المواقع لتخزين قدر من البيانات في المتصفح بهدف تسهيل استخدام تلك المواقع وإبداء استجابات ذكية لاختيارات وأفعال المستخدمين، وذلك بحفظ تفضيلاتهم وأحيانا بيانات حساباتهم. **cookies**

مُسَجِّل لوحة مفاتيح أداة تُزرع في حاسوب بغرض تسجيل ضربات أزرار لوحة المفاتيح أثناء استخدام الحاسوب على أمل أن تلتقط بيانات سرية يصعب الحصول عليها بوسائل أخرى، مثل كلمات السر في لحظة إدخالها، ثم إرسال ذلك السجل إلى الشخص الذي يتحكم في أداة التجسس هذه، إما عبر الشبكة أو بأن يسترجع بنفسه ملف السجلّ إن كان له نفاذ مادي إلى الحاسوب المستهدف. **keylogger**

شهادة رقمية وثيقة رقمية غير قابلة للتزييف تستخدم تقنية **التوقيع الرقمي** تفيد في اعتماد الوثائق الرقمية الأخرى والأكواد البرمجية وتوفير وسيلة للتحقق من أصالتها ومطابقتها للأصل الصادر عن الجهة الموقعة، وكذلك في استيثاق المراسلات بين الأفراد والنظم الحاسوبية. **digital certificate**

التوقيع الرقمي تقنية مبنية على التعمية بالمفتاح العلني تستخدم لمنع التلاعب بفحوى الوثائق والمراسلات الرقمية واكتشاف ذلك التلاعب إن حدث، وكذلك لكشف تزييف الوثائق والمراسلات وانتحال الهوية. **digital signature**

خادوم وسيط خادوم على الإنترنت يقوم بدور وسيط ما بين خادوم وعميل. تستعمل الخواديم لأغراض عديدة، منها تخفيف العبء على خواديم المحتوى والتطبيقات، وكذلك في تجاوز الرقابة على محتوى الإنترنت. **proxy server**

DISCLAIMER

Software and documentation in this collection of "NGO in a Box - Security Edition" is provided "as is" and we exclude and expressly disclaim all express and implied warranties or conditions of any kind, either express or implied, including, but not limited to, the implied warranties of merchant-ability and fitness for a particular purpose so far as such disclaimer is permitted. In no event shall Front Line Tactical Technology Collective or any agent or representatives there-of be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption), however caused under any theory of liability, arising in any way out of the use of or inability to make use of this software, even if advised of the possibility of such damage. Nothing in this disclaimer affects your statutory rights.